(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2001－352322
（P2001－352322A）
(43)公開日　平成13年12月21日(2001.12.21)

(51)Int.Cl.'	識別記号	ＦＩ		テーマコード'（参考）
Ｈ０４Ｌ　9/08		Ｇ０６Ｆ　12/14	３２０Ｂ	５Ｂ０１７
Ｇ０６Ｆ　12/14	３２０	Ｇ１１Ｂ　20/10	Ｈ	５Ｃ０５３
Ｇ１１Ｂ　20/10		Ｈ０４Ｌ　9/00	６０１Ａ	５Ｄ０４４
Ｈ０４Ｎ　5/91			６０１Ｄ	５Ｊ１０４
			６０１Ｅ	

審査請求　未請求　請求項の数58　ＯＬ　（全 70 頁）　最終頁に続く

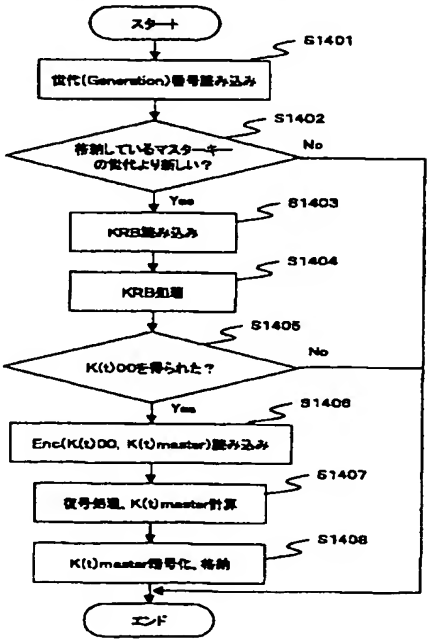
(21)出願番号　特願2000－243205(P2000－243205)
(22)出願日　平成12年８月10日(2000.8.10)
(31)優先権主張番号　特願2000－105328(P2000－105328)
(32)優先日　平成12年４月６日(2000.4.6)
(33)優先権主張国　日本（ＪＰ）

(71)出願人　000002185
ソニー株式会社
東京都品川区北品川６丁目７番35号
(72)発明者　浅野　智之
東京都品川区北品川６丁目７番35号　ソニー株式会社内
(72)発明者　大澤　義知
東京都品川区北品川６丁目７番35号　ソニー株式会社内
(74)代理人　100101801
弁理士　山田　英治　（外２名）

最終頁に続く

(54)【発明の名称】　情報記録装置、情報再生装置、情報記録方法、情報再生方法、および情報記録媒体、並びにプログラム提供媒体

(57)【要約】
【課題】　ツリー（木）構造の鍵配布構成によりキーの配布を実行して、効率的な鍵更新処理を可能とする。
【解決手段】　ツリー構造の鍵配布構成により、マスターキー、メディアキーの更新をキー更新ブロック（ＫＲＢ）とともに送信する。ＫＲＢは、ツリーのリーフを構成するデバイスにリーフキーおよび限定したノードキーを保有させた構成であり、特定のノードにより特定されるグループに特定のキー更新ブロック（ＫＲＢ）を生成して配布して、更新可能デバイスを限定することができる。グループに属さないデバイスは復号できず、キー配信の安全性が確保される。特に、世代管理を行なったマスターキーを使用するシステムにおいて、ＫＲＢによる更新マスターキーを配布する構成が実現される。



【特許請求の範囲】
【請求項１】記録媒体に情報を記録する情報記録装置において、
複数の異なる情報記録装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報記録装置固有のリーフキーとを保有し、
記録媒体に対する格納データの暗号化処理を実行する暗号処理手段を有し、
前記暗号処理手段は、
前記情報記録装置に内蔵した暗号化キー生成用データに基づいて暗号化キーを生成して前記記録媒体に格納するデータの暗号処理を実行する構成を有し、
前記暗号化キー生成用データは、前記ノードキーまたはリーフキーの少なくともいずれかを用いて更新可能なデータとして構成されていることを特徴とする情報記録装置。
【請求項２】前記暗号化キー生成用データは、複数の情報記録装置において共通なマスターキーであることを特徴とする請求項１に記載の情報記録装置。
【請求項３】前記暗号化キー生成用データは、特定の記録媒体に固有のメディアキーであることを特徴とする請求項１に記載の情報記録装置。
【請求項４】前記ノードキーは更新可能なキーとして構成され、更新処理に際しては更新ノードキーを下位階層のノードキーまたはリーフキーの少なくともいずれかを含むキーにより暗号化したキー更新ブロック（ＫＲＢ）を更新対象となるリーフの情報記録装置に配布する構成であり、
前記情報記録装置における前記暗号処理手段は、
前記更新ノードキーで暗号化処理した前記暗号化キー生成用データの更新データを受領し、
キー更新ブロック（ＫＲＢ）の暗号処理により、前記更新ノードキーを取得するとともに、該取得した更新ノードキーに基づいて前記暗号化キー生成用データの更新データを算出する構成を有することを特徴とする請求項１に記載の情報記録装置。
【請求項５】前記キー更新ブロック（ＫＲＢ）は、記録媒体に格納され、
前記暗号処理手段は、
前記記録媒体から読み出されたキー更新ブロック（ＫＲＢ）についての暗号処理を実行する構成であることを特徴とする請求項４に記載の情報記録装置。
【請求項６】前記暗号化キー生成用データは、更新情報としての世代番号が対応付けられた構成であり、
前記暗号処理部は、
前記記録媒体に対する暗号化データ格納時に、使用した前記暗号化キー生成用データの世代番号を記録時世代番号として前記記録媒体に格納する構成を有することを特徴とする請求項１に記載の情報記録装置。
【請求項７】前記情報記録装置は、さらに、
第1の暗号化キー生成用データに基づいて前記記録媒体に対する格納データの第1の暗号化キーを生成して該第1の暗号化キーに基づく暗号化処理を前記格納データに対して実行するとともに、前記第1の暗号化キー生成用データを前記記録媒体に格納する再生機器制限なしのデータ暗号処理と、
前記情報記録装置に内蔵した第２の暗号化キー生成用データに基づいて前記記録媒体に対する格納データの第２の暗号化キーを生成して該第２の暗号化キーに基づく暗号化処理を前記格納データに対して実行する再生機器制限ありのデータ暗号処理と、
を選択的に実行する構成を有することを特徴とする請求項１に記載の情報記録装置。
【請求項８】前記暗号処理手段は、
前記再生機器制限なしの暗号処理において、情報記録装置に格納された世代管理されたマスターキーと、記録媒体固有の記録媒体識別子であるディスクＩＤと、前記記録媒体に記録すべきデータ固有のタイトルキーと、情報記録装置の識別子であるデバイスＩＤとに基づいてタイトル固有キーを生成し、該タイトル固有キーに基づいて、前記第１の暗号化キーを生成し、
前記再生機器制限ありの暗号処理において、情報記録装置に格納された世代管理されたマスターキーと、記録媒体固有の記録媒体識別子であるディスクＩＤと、前記記録媒体に記録すべきデータ固有のタイトルキーと、情報記録装置の固有キーであるデバイス固有キーとに基づいてタイトル固有キーを生成し、該タイトル固有キーに基づいて、前記第２の暗号化キーを生成する構成であることを特徴とする請求項７に記載の情報記録装置。
【請求項９】前記情報記録装置は、さらに、
間欠的なトランスポートパケットから成るトランスポートストリームを構成する各パケットに受信時刻情報（ＡＴＳ）を付加するトランスポート・ストリーム処理手段を有し、
前記暗号処理手段は、
前記受信時刻情報（ＡＴＳ）の付加された1以上のパケットからなるブロックデータに対する暗号化キーとしてブロックキーを生成する構成を有し、
前記記録媒体に対する格納データの暗号処理においては、前記暗号化キー生成用データと前記受信時刻情報（ＡＴＳ）を含むブロックデータ固有の付加情報であるブロックシードとを含むデータに基づいて暗号化キーとしてのブロックキーを生成する構成を有することを特徴とする請求項１に記載の情報記録装置。
【請求項１０】前記暗号処理手段は、
前記記録媒体に対する格納データの暗号処理をＤＥＳアルゴリズムに従って実行する構成であることを特徴とする請求項１に記載の情報記録装置。
【請求項１１】前記情報記録装置は、
記録媒体に対する記録対象となる情報を受信するインタ

フェース手段を有し、
前記インタフェース手段は、データを構成するトランスポートストリームに含まれる各パケットに付加されたコピー制御情報を識別し、該コピー制御情報に基づいて記録媒体に対する記録実行の可否を制御する構成を有することを特徴とする請求項１に記載の情報記録装置。
【請求項１２】前記情報記録装置は、
記録媒体に対する記録対象となる情報を受信するインタフェース手段を有し、
前記インタフェース手段は、コピーを制御するためのコピー制御情報としての２ビットのＥＭＩ(Encryption Mode Indicator)を識別し、該ＥＭＩに基づいて記録媒体に対する記録実行の可否を制御する構成を有することを特徴とする請求項１に記載の情報記録装置。
【請求項１３】記録媒体から情報を再生する情報再生装置において、
複数の異なる情報再生装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報再生装置固有のリーフキーとを保有し、
記録媒体に格納された暗号データの復号処理を実行する暗号処理手段を有し、
前記暗号処理手段は、
前記情報記録装置に内蔵した復号キー生成用データに基づいて復号キーを生成して前記記録媒体に格納された暗号データの復号処理を実行する構成を有し、
前記復号キー生成用データは、前記ノードキーまたはリーフキーの少なくともいずれかを用いて更新可能なデータとして構成されていることを特徴とする情報再生装置。
【請求項１４】前記復号キー生成用データは、複数の情報記録装置において共通なマスターキーであることを特徴とする請求項１３に記載の情報再生装置。
【請求項１５】前記復号キー生成用データは、特定の記録媒体に固有のメディアキーであることを特徴とする請求項１３に記載の情報再生装置。
【請求項１６】前記ノードキーは更新可能なキーとして構成され、更新処理に際しては更新ノードキーを下位階層のノードキーまたはリーフキーの少なくともいずれかを含むキーにより暗号化したキー更新ブロック（ＫＲＢ）を更新対象となるリーフの情報再生装置に配布する構成であり、
前記情報記録装置における前記暗号処理手段は、
前記更新ノードキーで暗号化処理した前記復号キー生成用データの更新データを受領し、
キー更新ブロック（ＫＲＢ）の暗号処理により、前記更新ノードキーを取得するとともに、該取得した更新ノードキーに基づいて前記復号キー生成用データの更新データを算出する構成を有することを特徴とする請求項１３に記載の情報再生装置。
【請求項１７】前記キー更新ブロック（ＫＲＢ）は、記録媒体に格納され、
前記暗号処理手段は、
前記記録媒体から読み出されたキー更新ブロック（ＫＲＢ）についての暗号処理を実行する構成であることを特徴とする請求項１６に記載の情報再生装置。
【請求項１８】前記復号キー生成用データは、更新情報としての世代番号が対応付けられた構成であり、
前記暗号処理部は、
前記記録媒体からの暗号化データの復号時に、該暗号化データの暗号処理時に使用した暗号化キー生成用データの世代番号を前記記録媒体から読み取り、該読み取られた世代番号に対応する復号キー生成用データを使用して復号キーを生成する構成であることを特徴とする請求項１３に記載の情報再生装置。
【請求項１９】前記情報再生装置は、さらに、
前記記録媒体に格納された第1の復号キー生成用データに基づいて前記記録媒体に格納された暗号データに対する第1の復号キーを生成して該第1の復号キーに基づく復号処理を前記暗号データに対して実行する再生機器制限なしのデータ復号処理と、
前記情報記録装置に内蔵した第２の復号キー生成用データに基づいて前記記録媒体に格納された暗号データに対する第２の復号キーを生成して該第２の復号キーに基づく復号処理を前記暗号データに対して実行する再生機器制限ありのデータ復号処理と、
を選択的に実行する構成を有することを特徴とする請求項１３に記載の情報再生装置。
【請求項２０】前記暗号処理手段は、
前記再生機器制限なしの復号処理において、
情報記録装置に格納された世代管理されたマスターキーを取得するとともに、
記録媒体から、
記録媒体固有の記録媒体識別子であるディスクＩＤと、
復号対象データに固有のタイトルキーと、
暗号データを記録した情報記録装置の識別子であるデバイスＩＤ情報記録装置の識別子であるデバイスＩＤとを取得し、
前記マスターキー、ディスクＩＤ、タイトルキー、デバイスＩＤとに基づいてタイトル固有キーを生成し、該タイトル固有キーに基づいて、前記第１の復号キーを生成し、
前記再生機器制限ありの復号処理において、
情報記録装置に格納された世代管理されたマスターキーと、
情報記録装置に格納された情報記録装置の固有キーであるデバイス固有キーとを取得するとともに、
記録媒体から、
記録媒体固有の記録媒体識別子であるディスクＩＤと、
復号対象データに固有のタイトルキーとを取得し、
前記マスターキー、ディスクＩＤ、タイトルキー、デバ

イス固有キーとに基づいてタイトル固有キーを生成し、該タイトル固有キーに基づいて、前記第２の復号キーを生成する構成であることを特徴とする請求項１９に記載の情報再生装置。

【請求項２１】前記情報再生装置は、

前記暗号処理手段において復号されたブロックデータを構成する複数のトランスポートパケットの各々に付加された受信時刻情報（ＡＴＳ）に基づいてデータ出力制御を実行するトランスポート・ストリーム処理手段を有し、

前記暗号処理手段は、

前記受信時刻情報（ＡＴＳ）の付加された1以上のパケットからなるブロックデータに対する復号キーとしてブロックキーを生成する構成を有し、

前記記録媒体に格納された暗号データの復号処理においては、前記復号キー生成用データと前記受信時刻情報（ＡＴＳ）を含むブロックデータ固有の付加情報であるブロックシードとを含むデータに基づいて復号キーとしてのブロックキーを生成する構成を有することを特徴とする請求項１３に記載の情報再生装置。

【請求項２２】前記暗号処理手段は、

前記記録媒体に格納された暗号データの復号処理をＤＥＳアルゴリズムに従って実行する構成であることを特徴とする請求項１３に記載の情報再生装置。

【請求項２３】前記情報再生装置は、

記録媒体に対する記録対象となる情報を受信するインタフェース手段を有し、

前記インタフェース手段は、データを構成するトランスポートストリームに含まれる各パケットに付加されたコピー制御情報を識別し、該コピー制御情報に基づいて記録媒体からの再生実行の可否を制御する構成を有することを特徴とする請求項１３に記載の情報再生装置。

【請求項２４】前記情報再生装置は、

記録媒体に対する記録対象となる情報を受信するインタフェース手段を有し、

前記インタフェース手段は、コピーを制御するためのコピー制御情報としての２ビットのＥＭＩ(Encryption Mode Indicator)を識別し、該ＥＭＩに基づいて記録媒体からの再生実行の可否を制御する構成を有することを特徴とする請求項１３に記載の情報再生装置。

【請求項２５】記録媒体に情報を記録する情報記録方法において、

複数の異なる情報記録装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報記録装置固有のリーフキーの少なくともいずれかを用いて記録媒体に対する格納データの暗号化処理を実行する暗号化キーを生成するための暗号化キー生成用データの更新処理を実行する更新ステップと、

前記更新ステップにおいて更新された暗号化キー生成用データに基づいて暗号化キーを生成して前記記録媒体に格納するデータの暗号処理を実行する暗号処理ステップと、

を有することを特徴とする情報記録方法。

【請求項２６】前記暗号化キー生成用データは、複数の情報記録装置において共通なマスターキーであることを特徴とする請求項２５に記載の情報記録方法。

【請求項２７】前記暗号化キー生成用データは、特定の記録媒体に固有のメディアキーであることを特徴とする請求項２５に記載の情報記録方法。

【請求項２８】前記情報記録方法において、

前記ノードキーは更新可能なキーとして構成され、更新処理に際しては更新ノードキーを下位階層のノードキーまたはリーフキーの少なくともいずれかを含むキーにより暗号化したキー更新ブロック（ＫＲＢ）を更新対象となるリーフの情報記録装置に配布する構成であり、

前記更新ステップは、

前記キー更新ブロック（ＫＲＢ）の暗号処理により、前記更新ノードキーを取得する更新ノードキー取得ステップと、

取得した更新ノードキーに基づいて前記暗号化キー生成用データの更新データを算出する更新データ取得ステップと、

を含むことを特徴とする請求項２５に記載の情報記録方法。

【請求項２９】前記暗号化キー生成用データは、更新情報としての世代番号が対応付けられた構成であり、

前記暗号処理ステップは、さらに、

前記記録媒体に対する暗号化データ格納時に、使用した前記暗号化キー生成用データの世代番号を記録時世代番号として前記記録媒体に格納するステップを含むことを特徴とする請求項２５に記載の情報記録方法。

【請求項３０】前記暗号処理ステップは、

第1の暗号化キー生成用データに基づいて前記記録媒体に対する格納データの第1の暗号化キーを生成して該第1の暗号化キーに基づく暗号化処理を前記格納データに対して実行するとともに、前記第1の暗号化キー生成用データを前記記録媒体に格納する再生機器制限なしのデータ暗号処理と、

前記情報記録装置に内蔵した第２の暗号化キー生成用データに基づいて前記記録媒体に対する格納データの第２の暗号化キーを生成して該第２の暗号化キーに基づく暗号化処理を前記格納データに対して実行する再生機器制限ありのデータ暗号処理と、

を選択的に実行することを特徴とする請求項２５に記載の情報記録方法。

【請求項３１】前記暗号処理ステップは、

前記再生機器制限なしの暗号処理において、情報記録装置に格納された世代管理されたマスターキーと、記録媒体固有の記録媒体識別子であるディスクＩＤと、前記記録媒体に記録すべきデータ固有のタイトルキーと、情報

記録装置の識別子であるデバイスＩＤとに基づいてタイトル固有キーを生成し、該タイトル固有キーに基づいて、前記第１の暗号化キーを生成し、
前記再生機器制限ありの暗号処理において、情報記録装置に格納された世代管理されたマスターキーと、記録媒体固有の記録媒体識別子であるディスクＩＤと、前記記録媒体に記録すべきデータ固有のタイトルキーと、情報記録装置の固有キーであるデバイス固有キーとに基づいてタイトル固有キーを生成し、該タイトル固有キーに基づいて、前記第２の暗号化キーを生成する構成であることを特徴とする請求項３０に記載の情報記録方法。
【請求項３２】前記情報記録方法は、さらに、
間欠的なトランスポートパケットから成るトランスポートストリームを構成する各パケットに受信時刻情報（ＡＴＳ）を付加するトランスポート・ストリーム処理ステップを有し、
前記暗号処理ステップは、
前記受信時刻情報（ＡＴＳ）の付加された1以上のパケットからなるブロックデータに対する暗号化キーとしてブロックキーを生成し、
前記記録媒体に対する格納データの暗号処理においては、前記暗号化キー生成用データと前記受信時刻情報（ＡＴＳ）を含むブロックデータ固有の付加情報であるブロックシードとを含むデータに基づいて暗号化キーとしてのブロックキーを生成することを特徴とする請求項２５に記載の情報記録方法。
【請求項３３】前記暗号処理ステップは、
前記記録媒体に対する格納データの暗号処理をＤＥＳアルゴリズムに従って実行することを特徴とする請求項２５に記載の情報記録方法。
【請求項３４】前記情報記録方法は、さらに、
データを構成するトランスポートストリームに含まれる各パケットに付加されたコピー制御情報を識別し、該コピー制御情報に基づいて記録媒体に対する記録実行の可否を制御することを特徴とする請求項２５に記載の情報記録方法。
【請求項３５】前記情報記録方法は、さらに、
コピーを制御するためのコピー制御情報としての２ビットのＥＭＩ(Encryption Mode Indicator)を識別し、該ＥＭＩに基づいて記録媒体に対する記録実行の可否を制御することを特徴とする請求項２５に記載の情報記録方法。
【請求項３６】記録媒体から情報を再生する情報再生方法であり、
複数の異なる情報再生装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報再生装置固有のリーフキーの少なくともいずれかを用いて記録媒体に格納された暗号データの復号処理を実行する復号キーを生成するための復号キー生成用データの更新処理を実行する更新ステップと、
前記更新ステップにおいて更新された復号キー生成用データに基づいて復号キーを生成して前記記録媒体に格納された暗号データの復号処理を実行する復号処理ステップと、
を有することを特徴とする情報再生方法。
【請求項３７】前記復号キー生成用データは、複数の情報記録装置において共通なマスターキーであることを特徴とする請求項３６に記載の情報再生方法。
【請求項３８】前記復号キー生成用データは、特定の記録媒体に固有のメディアキーであることを特徴とする請求項３６に記載の情報再生方法。
【請求項３９】前記情報再生方法において、
前記ノードキーは更新可能なキーとして構成され、更新処理に際しては更新ノードキーを下位階層のノードキーまたはリーフキーの少なくともいずれかを含むキーにより暗号化したキー更新ブロック（ＫＲＢ）を更新対象となるリーフの情報再生装置に配布する構成であり、
前記更新ステップは、
前記キー更新ブロック（ＫＲＢ）の暗号処理により、前記更新ノードキーを取得する更新ノードキー取得ステップと、
取得した更新ノードキーに基づいて前記復号キー生成用データの更新データを算出する更新データ取得ステップと、
を含むことを特徴とする請求項３６に記載の情報再生方法。
【請求項４０】前記復号キー生成用データは、更新情報としての世代番号が対応付けられた構成であり、
前記復号処理ステップは、
前記記録媒体からの暗号化データの復号時に、該暗号化データの暗号処理時に使用した暗号化キー生成用データの世代番号を前記記録媒体から読み取り、該読み取られた世代番号に対応する復号キー生成用データを使用して復号キーを生成することを特徴とする請求項３６に記載の情報再生方法。
【請求項４１】前記情報再生方法は、さらに、
前記記録媒体に格納された第1の復号キー生成用データに基づいて前記記録媒体に格納された暗号データに対する第1の復号キーを生成して該第1の復号キーに基づく復号処理を前記暗号データに対して実行する再生機器制限なしのデータ復号処理と、
前記情報記録装置に内蔵した第２の復号キー生成用データに基づいて前記記録媒体に格納された暗号データに対する第２の復号キーを生成して該第２の復号キーに基づく復号処理を前記暗号データに対して実行する再生機器制限ありのデータ復号処理と、
を選択的に実行することを特徴とする請求項３６に記載の情報再生方法。
【請求項４２】前記復号処理ステップは、
前記再生機器制限なしの復号処理において、

情報記録装置に格納された世代管理されたマスターキーを取得するとともに、
記録媒体から、
記録媒体固有の記録媒体識別子であるディスクＩＤと、
復号対象データに固有のタイトルキーと、
暗号データを記録した情報記録装置の識別子であるデバイスＩＤ情報記録装置の識別子であるデバイスＩＤとを取得し、
前記マスターキー、ディスクＩＤ、タイトルキー、デバイスＩＤとに基づいてタイトル固有キーを生成し、該タイトル固有キーに基づいて、前記第１の復号キーを生成し、
前記再生機器制限ありの復号処理において、
情報記録装置に格納された世代管理されたマスターキーと、
情報記録装置に格納された情報記録装置の固有キーであるデバイス固有キーとを取得するとともに、
記録媒体から、
記録媒体固有の記録媒体識別子であるディスクＩＤと、
復号対象データに固有のタイトルキーとを取得し、
前記マスターキー、ディスクＩＤ、タイトルキー、デバイス固有キーとに基づいてタイトル固有キーを生成し、該タイトル固有キーに基づいて、前記第２の復号キーを生成することを特徴とする請求項４１に記載の情報再生方法。

【請求項４３】前記情報再生方法において、
情報再生装置は、復号されたブロックデータを構成する複数のトランスポートパケットの各々に付加された受信時刻情報（ＡＴＳ）に基づいてデータ出力制御を実行するトランスポート・ストリーム処理手段を有し、
前記復号処理ステップは、
前記受信時刻情報（ＡＴＳ）の付加された1以上のパケットからなるブロックデータに対する復号キーとしてブロックキーを生成し、
前記記録媒体に格納された暗号データの復号処理においては、前記復号キー生成用データと前記受信時刻情報（ＡＴＳ）を含むブロックデータ固有の付加情報であるブロックシードとを含むデータに基づいて復号キーとしてのブロックキーを生成することを特徴とする請求項３６に記載の情報再生方法。

【請求項４４】前記復号処理ステップは、
前記記録媒体に格納された暗号データの復号処理をＤＥＳアルゴリズムに従って実行することを特徴とする請求項３６に記載の情報再生方法。

【請求項４５】前記情報再生方法は、さらに、
データを構成するトランスポートストリームに含まれる各パケットに付加されたコピー制御情報を識別し、該コピー制御情報に基づいて記録媒体に格納されたデータの再生実行の可否を制御することを特徴とする請求項３６に記載の情報再生方法。

【請求項４６】前記情報再生方法は、さらに、
コピーを制御するためのコピー制御情報としての２ビットのＥＭＩ(Encryption Mode Indicator)を識別し、該ＥＭＩに基づいて記録媒体に格納されたデータの再生実行の可否を制御することを特徴とする請求項３６に記載の情報再生方法。

【請求項４７】情報を記録可能な情報記録媒体であって、
複数の異なる情報記録装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報記録装置固有のリーフキーに含まれる更新ノードキーを下位階層のノードキーまたはリーフキーの少なくともいずれかを含むキーにより暗号化したキー更新ブロック（ＫＲＢ）を格納したことを特徴とする情報記録媒体。

【請求項４８】前記情報記録媒体は、さらに、
情報記録装置において記録媒体に格納するデータの暗号化処理に用いる暗号化キーを生成するための暗号化キー生成用データを前記更新ノードキーによって暗号化したデータを含むことを特徴とする請求項４７に記載の情報記録媒体。

【請求項４９】前記情報記録媒体は、さらに、
情報再生装置において記録媒体に格納された暗号データの復号処理に用いる復号キーを生成するための復号キー生成用データを前記更新ノードキーによって暗号化したデータを含むことを特徴とする請求項４７に記載の情報記録媒体。

【請求項５０】前記情報記録媒体は、さらに、暗号化キー生成用データまたは復号キー生成用データに関する世代情報を格納した構成であることを特徴とする請求項４７に記載の情報記録媒体。

【請求項５１】情報記録媒体を製造する記録媒体製造装置であり、
複数の異なる情報記録装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報記録装置固有のリーフキーに含まれる更新ノードキーを下位階層のノードキーまたはリーフキーの少なくともいずれかを含むキーにより暗号化したキー更新ブロック（ＫＲＢ）を格納するメモリと、
前記メモリに格納されたキー更新ブロック（ＫＲＢ）の前記記録媒体に対する書き込み制御を実行する制御部と、
を有することを特徴とする記録媒体製造装置。

【請求項５２】前記メモリには、さらに、
記録媒体識別子と、暗号化された暗号化キー生成用データまたは暗号化された復号キー生成用データの少なくともいずれかを格納し、
前記制御部は、前記記録媒体識別子、暗号化された暗号化キー生成用データ、または暗号化された復号キー生成用データの少なくともいずれかについて、前記記録媒体に対する書き込み制御を実行する構成であることを特徴

とする請求項５１に記載の記録媒体製造装置。
【請求項５３】前記メモリには、さらに、
暗号化キー生成用データまたは復号キー生成用データに関する世代情報を格納し、
前記制御部は、前記世代情報の前記記録媒体に対する書き込み制御を実行する構成であることを特徴とする請求項５１に記載の記録媒体製造装置。
【請求項５４】記録媒体を製造する記録媒体製造方法であり、
複数の異なる情報記録装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報記録装置固有のリーフキーに含まれる更新ノードキーを下位階層のノードキーまたはリーフキーの少なくともいずれかを含むキーにより暗号化したキー更新ブロック（ＫＲＢ）をメモリに格納するステップと、
前記メモリに格納されたキー更新ブロック（ＫＲＢ）の前記記録媒体に対する書き込みを実行するステップと、
を有することを特徴とする記録媒体製造方法。
【請求項５５】前記記録媒体製造方法において、
前記メモリに、さらに、
記録媒体識別子、暗号化された暗号化キー生成用データ、または暗号化された復号キー生成用データの少なくともいずれかを格納し、
前記記録媒体識別子、暗号化された暗号化キー生成用データ、または暗号化された復号キー生成用データの少なくともいずれかについて、前記記録媒体に対する書き込みを実行することを特徴とする請求項５４に記載の記録媒体製造方法。
【請求項５６】前記記録媒体製造方法において、
前記メモリに、さらに、
暗号化キー生成用データまたは復号キー生成用データに関する世代情報を格納し、
前記制御部は、前記世代情報の前記記録媒体に対する書き込みを実行することを特徴とする請求項５４に記載の記録媒体製造方法。
【請求項５７】記録媒体に情報を記録する情報記録処理をコンピュータ・システム上で実行せしめるコンピュータ・プログラムを提供するプログラム提供媒体であって、前記コンピュータ・プログラムは、
複数の異なる情報記録装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報記録装置固有のリーフキーの少なくともいずれかを用いて記録媒体に対する格納データの暗号化処理を実行する暗号化キーを生成するための暗号化キー生成用データの更新処理を実行する更新ステップと、
前記更新ステップにおいて更新された暗号化キー生成用データに基づいて暗号化キーを生成して前記記録媒体に格納するデータの暗号処理を実行する暗号処理ステップと、
を有することを特徴とするプログラム提供媒体。
【請求項５８】記録媒体に格納された情報を再生する情報再生処理をコンピュータ・システム上で実行せしめるコンピュータ・プログラムを提供するプログラム提供媒体であって、前記コンピュータ・プログラムは、
複数の異なる情報再生装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報再生装置固有のリーフキーの少なくともいずれかを用いて記録媒体に格納された暗号データの復号処理を実行する復号キーを生成するための復号キー生成用データの更新処理を実行する更新ステップと、
前記更新ステップにおいて更新された復号キー生成用データに基づいて復号キーを生成して前記記録媒体に格納された暗号データの復号処理を実行する復号処理ステップと、
を有することを特徴とするプログラム提供媒体。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、情報記録装置、情報再生装置、情報記録方法、情報再生方法、および情報記録媒体、並びにプログラム提供媒体に関し、特に、木構造の階層的鍵配信方式を用いることにより、メッセージ量を小さく押さえて、マスターキーあるいはメディアキー等の鍵更新におけるデータ配信の負荷を軽減することを可能とした構成を提供する。具体的には、各記録再生器機器をｎ分木の各葉（リーフ）に配置した構成の鍵配信方法を用い、記録媒体もしくは通信回線を介して、コンテンツデータの記録媒体への記録もしくは記録媒体からの再生に必要な鍵（マスターキーもしくはメディアキー）を配信し、これを用いて各装置がコンテンツデータの記録、再生を行う構成とした情報記録装置、情報再生装置、情報記録方法、情報再生方法、および情報記録媒体、並びにプログラム提供媒体に関する。
【０００２】
【従来の技術】ディジタル信号処理技術の進歩、発展に伴い、近年においては、情報を、ディジタル的に記録する記録装置や記録媒体が普及しつつある。このようなディジタル記録装置および記録媒体によれば、例えば画像や音声を劣化させることなく記録、再生を繰り返すことができる。このようにディジタルデータは画質や音質を維持したまま何度もコピーを繰り返し実行することができるため、コピーが違法に行われた記録媒体が市場に流通することになると、音楽、映画等各種コンテンツの著作権者、あるいは正当な販売権者等の利益が害されることになる。昨今では、このようなディジタルデータの不正なコピーを防ぐため、ディジタル記録装置および記録媒体に違法なコピーを防止するための様々な仕組み（システム）が導入されている。
【０００３】例えば、ＭＤ（ミニディスク）（ＭＤは商標）装置において、違法なコピーを防止する方法として、ＳＣＭＳ(Serial Copy Management System)が採用

されている。ＳＣＭＳは、データ再生側において、オーディオデータとともにＳＣＭＳ信号をディジタルインタフェース（ＤＩＦ）から出力し、データ記録側において、再生側からのＳＣＭＳ信号に基づいて、再生側からのオーディオデータの記録を制御することにより違法なコピーを防止するシステムである。

【０００４】具体的にはＳＣＭＳ信号は、オーディオデータが、何度でもコピーが許容されるコピーフリー（copy free）のデータであるか、１度だけコピーが許されている（copy once allowed）データであるか、またはコピーが禁止されている（copy prohibited）データであるかを表す信号である。データ記録側において、ＤＩＦからオーディオデータを受信すると、そのオーディオデータとともに送信されるＳＣＭＳ信号を検出する。そして、ＳＣＭＳ信号が、コピーフリー（copy free）となっている場合には、オーディオデータをＳＣＭＳ信号とともにミニディスクに記録する。また、ＳＣＭＳ信号が、コピーを１度のみ許可（copy once allowed）となっている場合には、ＳＣＭＳ信号をコピー禁止（copy prohibited）に変更して、オーディオデータとともに、ミニディスクに記録する。さらに、ＳＣＭＳ信号が、コピー禁止（copy prohibited）となっている場合には、オーディオデータの記録を行わない。このようなＳＣＭＳを使用した制御を行なうことで、ミニディスク装置では、ＳＣＭＳによって、著作権を有するオーディオデータが、違法にコピーされるのを防止するようになっている。

【０００５】しかしながら、ＳＣＭＳは上述のようにＳＣＭＳ信号に基づいて再生側からのオーディオデータの記録を制御する構成をデータを記録する機器自体が有していることが前提であるため、ＳＣＭＳの制御を実行する構成を持たないミニディスク装置が製造された場合には、対処するのが困難となる。そこで、例えば、ＤＶＤプレーヤでは、コンテンツ・スクランブルシステムを採用することにより、著作権を有するデータの違法コピーを防止する構成となっている。

【０００６】コンテンツ・スクランブルシステムでは、ＤＶＤ－ＲＯＭ(Read Only Memory)に、ビデオデータやオーディオデータ等が暗号化されて記録されており、その暗号化されたデータを復号するのに用いるキー（復号鍵）が、ライセンスを受けたＤＶＤプレーヤに与えられる。ライセンスは、不正コピーを行わない等の所定の動作規定に従うように設計されたＤＶＤプレーヤに対して与えられる。従って、ライセンスを受けたＤＶＤプレーヤでは、与えられたキーを利用して、ＤＶＤ－ＲＯＭに記録された暗号化データを復号することにより、ＤＶＤ－ＲＯＭから画像や音声を再生することができる。

【０００７】一方、ライセンスを受けていないＤＶＤプレーヤは、暗号化されたデータを復号するためのキーを有していないため、ＤＶＤ－ＲＯＭに記録された暗号化データの復号を行うことができない。このように、コンテンツ・スクランブルシステム構成では、ライセンス時に要求される条件を満たしていないＤＶＤプレーヤは、ディジタルデータを記録したＤＶＤ－ＲＯＭの再生を行なえないことになり、不正コピーが防止されるようになっている。

【０００８】しかしながら、ＤＶＤ－ＲＯＭで採用されているコンテンツ・スクランブルシステムは、ユーザによるデータの書き込みが不可能な記録媒体（以下、適宜、ＲＯＭメディアという）を対象としており、ユーザによるデータの書き込みが可能な記録媒体（以下、適宜、ＲＡＭメディアという）への適用については考慮されていない。

【０００９】即ち、ＲＯＭメディアに記録されたデータが暗号化されていても、その暗号化されたデータを、そのまま全部、ＲＡＭメディアにコピーした場合には、ライセンスを受けた正当な装置で再生可能な、いわゆる海賊版を作成することができてしまう。

【００１０】そこで、本出願人は、先の特許出願、特開平１１－２２４４６１号公報（特願平１０－２５３１０号）において、個々の記録媒体を識別する為の情報（以下、媒体識別情報と記述する）を、他のデータとともに記録媒体に記録し、この媒体識別情報のライセンスを受けた装置であることを条件として、その条件が満たされた場合にのみ記録媒体の媒体識別情報へのアクセスが可能となる構成を提案した。

【００１１】この方法では、記録媒体上のデータは、媒体識別情報とライセンスを受けることにより得られる秘密キー（マスターキー）により暗号化され、ライセンスを受けていない装置が、この暗号化されたデータを読み出したとしても、意味のあるデータを得ることができないようになっている。なお、装置はライセンスを受ける際、不正な複製（違法コピー）ができないように、その動作が規定される。

【００１２】ライセンスを受けていない装置は、媒体識別情報にアクセスできず、また、媒体識別情報は個々の媒体毎に個別の値となっているため、ライセンスを受けていない装置が、記録媒体に記録されている、暗号化されたデータのすべてを新たな記録媒体に複製したとしても、そのようにして作成された記録媒体に記録されたデータは、ライセンスを受けていない装置は勿論、ライセンスを受けた装置においても、正しく復号することができないから、実質的に、違法コピーが防止されることになる。

【００１３】

【発明が解決しようとする課題】ところで、上記の構成においては、ライセンスを受けた装置において格納されるマスターキーは全機器において共通であるのが一般的である。このように複数の機器に対して共通のマスターキーを格納するのは、１つの機器で記録された媒体を他

の機器で再生可能とする（インターオペラビリティを確保する）ために必要な条件であるからである。

【００１４】しかし、この方式においては、攻撃者が１つの機器の攻撃に成功し、マスターキーを取出した場合、全システムにおいて暗号化されて記録されているデータを復号することができてしまい、システム全体が崩壊する。これを防ぐためには、ある機器が攻撃されてマスターキーが露呈したことが発覚した場合、マスターキーを新たなものに更新し、攻撃に屈した機器以外の全機器に新たに更新されたマスターキーを与えることが必要になる。この構成を実現する一番単純な方式としては、個々の機器に固有の鍵（デバイスキー）を与えておき、新たなマスターキーを個々のデバイスキーで暗号化した値を用意し、記録媒体を介して機器に伝送する方式が考えられるが、機器の台数に比例して伝送すべき全メッセージ量が増加するという問題がある。

【００１５】本発明は、上述の問題点を解決することを目的とするものであり、木構造の階層的鍵配信方式を用いることにより、メッセージ量を小さく押さえて、新たな更新キーの配信の負荷を軽減することを可能とした構成を提供する。すなわち、各機器をｎ分木の各葉（リーフ）に配置した構成の鍵配信方法を用い、記録媒体もしくは通信回線を介して、コンテンツデータの記録媒体への記録もしくは記録媒体からの再生に必要な鍵（マスターキーもしくはメディアキー）を配信し、これを用いて各装置がコンテンツデータの記録、再生を行う構成とした情報記録装置、情報再生装置、情報記録方法、情報再生方法、および情報記録媒体、並びにプログラム提供媒体を提供することを目的とする。

【００１６】

【課題を解決するための手段】本発明の第１の側面は、記録媒体に情報を記録する情報記録装置において、複数の異なる情報記録装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報記録装置固有のリーフキーとを保有し、記録媒体に対する格納データの暗号化処理を実行する暗号処理手段を有し、前記暗号処理手段は、前記情報記録装置に内蔵した暗号化キー生成用データに基づいて暗号化キーを生成して前記記録媒体に格納するデータの暗号処理を実行する構成を有し、前記暗号化キー生成用データは、前記ノードキーまたはリーフキーの少なくともいずれかを用いて更新可能なデータとして構成されていることを特徴とする情報記録装置にある。

【００１７】さらに、本発明の情報記録装置の一実施態様において、前記暗号化キー生成用データは、複数の情報記録装置において共通なマスターキーであることを特徴とする。

【００１８】さらに、本発明の情報記録装置の一実施態様において、前記暗号化キー生成用データは、特定の記録媒体に固有のメディアキーであることを特徴とする。

【００１９】さらに、本発明の情報記録装置の一実施態様において、前記ノードキーは更新可能なキーとして構成され、更新処理に際しては更新ノードキーを下位階層のノードキーまたはリーフキーの少なくともいずれかを含むキーにより暗号化したキー更新ブロック（ＫＲＢ）を更新対象となるリーフの情報記録装置に配布する構成であり、前記情報記録装置における前記暗号処理手段は、前記更新ノードキーで暗号化処理した前記暗号化キー生成用データの更新データを受領し、キー更新ブロック（ＫＲＢ）の暗号処理により、前記更新ノードキーを取得するとともに、該取得した更新ノードキーに基づいて前記暗号化キー生成用データの更新データを算出する構成を有することを特徴とする。

【００２０】さらに、本発明の情報記録装置の一実施態様において、前記キー更新ブロック（ＫＲＢ）は、記録媒体に格納され、前記暗号処理手段は、前記記録媒体から読み出されたキー更新ブロック（ＫＲＢ）についての暗号処理を実行する構成であることを特徴とする。

【００２１】さらに、本発明の情報記録装置の一実施態様において、前記暗号化キー生成用データは、更新情報としての世代番号が対応付けられた構成であり、前記暗号処理部は、前記記録媒体に対する暗号化データ格納時に、使用した前記暗号化キー生成用データの世代番号を記録時世代番号として前記記録媒体に格納する構成を有することを特徴とする。

【００２２】さらに、本発明の情報記録装置の一実施態様において、第1の暗号化キー生成用データに基づいて前記記録媒体に対する格納データの第1の暗号化キーを生成して該第1の暗号化キーに基づく暗号化処理を前記格納データに対して実行するとともに、前記第1の暗号化キー生成用データを前記記録媒体に格納する再生機器制限なしのデータ暗号処理と、前記情報記録装置に内蔵した第２の暗号化キー生成用データに基づいて前記記録媒体に対する格納データの第２の暗号化キーを生成して該第２の暗号化キーに基づく暗号化処理を前記格納データに対して実行する再生機器制限ありのデータ暗号処理と、を選択的に実行する構成を有することを特徴とする。

【００２３】さらに、本発明の情報記録装置の一実施態様において、前記暗号処理手段は、前記再生機器制限なしの暗号処理において、情報記録装置に格納された世代管理されたマスターキーと、記録媒体固有の記録媒体識別子であるディスクＩＤと、前記記録媒体に記録すべきデータ固有のタイトルキーと、情報記録装置の識別子であるデバイスＩＤとに基づいてタイトル固有キーを生成し、該タイトル固有キーに基づいて、前記第１の暗号化キーを生成し、前記再生機器制限ありの暗号処理において、情報記録装置に格納された世代管理されたマスターキーと、記録媒体固有の記録媒体識別子であるディスクＩＤと、前記記録媒体に記録すべきデータ固有のタイト

ルキーと、情報記録装置の固有キーであるデバイス固有キーとに基づいてタイトル固有キーを生成し、該タイトル固有キーに基づいて、前記第２の暗号化キーを生成する構成であることを特徴とする。

【００２４】さらに、本発明の情報記録装置の一実施態様において、間欠的なトランスポートパケットから成るトランスポートストリームを構成する各パケットに受信時刻情報（ＡＴＳ）を付加するトランスポート・ストリーム処理手段を有し、前記暗号処理手段は、前記受信時刻情報（ＡＴＳ）の付加された1以上のパケットからなるブロックデータに対する暗号化キーとしてブロックキーを生成する構成を有し、前記記録媒体に対する格納データの暗号処理においては、前記暗号化キー生成用データと前記受信時刻情報（ＡＴＳ）を含むブロックデータ固有の付加情報であるブロックシードとを含むデータに基づいて暗号化キーとしてのブロックキーを生成する構成を有することを特徴とする。

【００２５】さらに、本発明の情報記録装置の一実施態様において、前記暗号処理手段は、前記記録媒体に対する格納データの暗号処理をＤＥＳアルゴリズムに従って実行する構成であることを特徴とする。

【００２６】さらに、本発明の情報記録装置の一実施態様において、記録媒体に対する記録対象となる情報を受信するインタフェース手段を有し、前記インタフェース手段は、データを構成するトランスポートストリームに含まれる各パケットに付加されたコピー制御情報を識別し、該コピー制御情報に基づいて記録媒体に対する記録実行の可否を制御する構成を有することを特徴とする。

【００２７】さらに、本発明の情報記録装置の一実施態様において、記録媒体に対する記録対象となる情報を受信するインタフェース手段を有し、前記インタフェース手段は、コピーを制御するためのコピー制御情報としての2ビットのＥＭＩ(Encryption Mode Indicator)を識別し、該ＥＭＩに基づいて記録媒体に対する記録実行の可否を制御する構成を有することを特徴とする。

【００２８】さらに、本発明の第２の側面は、記録媒体から情報を再生する情報再生装置において、複数の異なる情報再生装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報再生装置固有のリーフキーとを保有し、記録媒体に格納された暗号データの復号処理を実行する暗号処理手段を有し、前記暗号処理手段は、前記情報記録装置に内蔵した復号キー生成用データに基づいて復号キーを生成して前記記録媒体に格納された暗号データの復号処理を実行する構成を有し、前記復号キー生成用データは、前記ノードキーまたはリーフキーの少なくともいずれかを用いて更新可能なデータとして構成されていることを特徴とする情報再生装置にある。

【００２９】さらに、本発明の情報再生装置の一実施態様において、前記復号キー生成用データは、複数の情報記録装置において共通なマスターキーであることを特徴とする。

【００３０】さらに、本発明の情報再生装置の一実施態様において、前記復号キー生成用データは、特定の記録媒体に固有のメディアキーであることを特徴とする。

【００３１】さらに、本発明の情報再生装置の一実施態様において、前記ノードキーは更新可能なキーとして構成され、更新処理に際しては更新ノードキーを下位階層のノードキーまたはリーフキーの少なくともいずれかを含むキーにより暗号化したキー更新ブロック（ＫＲＢ）を更新対象となるリーフの情報再生装置に配布する構成であり、前記情報記録装置における前記暗号処理手段は、前記更新ノードキーで暗号化処理した前記復号キー生成用データの更新データを受領し、キー更新ブロック（ＫＲＢ）の暗号処理により、前記更新ノードキーを取得するとともに、該取得した更新ノードキーに基づいて前記復号キー生成用データの更新データを算出する構成を有することを特徴とする。

【００３２】さらに、本発明の情報再生装置の一実施態様において、前記キー更新ブロック（ＫＲＢ）は、記録媒体に格納され、前記暗号処理手段は、前記記録媒体から読み出されたキー更新ブロック（ＫＲＢ）についての暗号処理を実行する構成であることを特徴とする。

【００３３】さらに、本発明の情報再生装置の一実施態様において、前記復号キー生成用データは、更新情報としての世代番号が対応付けられた構成であり、前記暗号処理部は、前記記録媒体からの暗号化データの復号時に、該暗号化データの暗号処理時に使用した暗号化キー生成用データの世代番号を前記記録媒体から読み取り、該読み取られた世代番号に対応する復号キー生成用データを使用して復号キーを生成する構成であることを特徴とする。

【００３４】さらに、本発明の情報再生装置の一実施態様において、前記記録媒体に格納された第1の復号キー生成用データに基づいて前記記録媒体に格納された暗号データに対する第1の復号キーを生成して該第1の復号キーに基づく復号処理を前記暗号データに対して実行する再生機器制限なしのデータ復号処理と、前記情報記録装置に内蔵した第２の復号キー生成用データに基づいて前記記録媒体に格納された暗号データに対する第２の復号キーを生成して該第２の復号キーに基づく復号処理を前記暗号データに対して実行する再生機器制限ありのデータ復号処理と、を選択的に実行する構成を有することを特徴とする。

【００３５】さらに、本発明の情報再生装置の一実施態様において、前記暗号処理手段は、前記再生機器制限なしの復号処理において、情報記録装置に格納された世代管理されたマスターキーを取得するとともに、記録媒体から、記録媒体固有の記録媒体識別子であるディスクＩＤと、復号対象データに固有のタイトルキーと、暗号デ

ータを記録した情報記録装置の識別子であるデバイスＩＤ情報記録装置の識別子であるデバイスＩＤとを取得し、前記マスターキー、ディスクＩＤ、タイトルキー、デバイスＩＤとに基づいてタイトル固有キーを生成し、該タイトル固有キーに基づいて、前記第１の復号キーを生成し、前記再生機器制限ありの復号処理において、情報記録装置に格納された世代管理されたマスターキーと、情報記録装置に格納された情報記録装置の固有キーであるデバイス固有キーとを取得するとともに、記録媒体から、記録媒体固有の記録媒体識別子であるディスクＩＤと、復号対象データに固有のタイトルキーとを取得し、前記マスターキー、ディスクＩＤ、タイトルキー、デバイス固有キーとに基づいてタイトル固有キーを生成し、該タイトル固有キーに基づいて、前記第２の復号キーを生成する構成であることを特徴とする。

【００３６】さらに、本発明の情報再生装置の一実施態様において、前記暗号処理手段において復号されたブロックデータを構成する複数のトランスポートパケットの各々に付加された受信時刻情報（ＡＴＳ）に基づいてデータ出力制御を実行するトランスポート・ストリーム処理手段を有し、前記暗号処理手段は、前記受信時刻情報（ＡＴＳ）の付加された1以上のパケットからなるブロックデータに対する復号キーとしてブロックキーを生成する構成を有し、前記記録媒体に格納された暗号データの復号処理においては、前記復号キー生成用データと前記受信時刻情報（ＡＴＳ）を含むブロックデータ固有の付加情報であるブロックシードとを含むデータに基づいて復号キーとしてのブロックキーを生成する構成を有することを特徴とする。

【００３７】さらに、本発明の情報再生装置の一実施態様において、前記暗号処理手段は、前記記録媒体に格納された暗号データの復号処理をＤＥＳアルゴリズムに従って実行する構成であることを特徴とする。

【００３８】さらに、本発明の情報再生装置の一実施態様において、前記情報再生装置は、記録媒体に対する記録対象となる情報を受信するインタフェース手段を有し、前記インタフェース手段は、データを構成するトランスポートストリームに含まれる各パケットに付加されたコピー制御情報を識別し、該コピー制御情報に基づいて記録媒体からの再生実行の可否を制御する構成を有することを特徴とする。

【００３９】さらに、本発明の情報再生装置の一実施態様において、記録媒体に対する記録対象となる情報を受信するインタフェース手段を有し、前記インタフェース手段は、コピーを制御するためのコピー制御情報としての２ビットのＥＭＩ(Encryption Mode Indicator)を識別し、該ＥＭＩに基づいて記録媒体からの再生実行の可否を制御する構成を有することを特徴とする。

【００４０】さらに、本発明の第３の側面は、記録媒体に情報を記録する情報記録方法において、複数の異なる情報記録装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報記録装置固有のリーフキーの少なくともいずれかを用いて記録媒体に対する格納データの暗号化処理を実行する暗号化キーを生成するための暗号化キー生成用データの更新処理を実行する更新ステップと、前記更新ステップにおいて更新された暗号化キー生成用データに基づいて暗号化キーを生成して前記記録媒体に格納するデータの暗号処理を実行する暗号処理ステップと、を有することを特徴とする情報記録方法にある。

【００４１】さらに、本発明の情報記録方法の一実施態様において、前記暗号化キー生成用データは、複数の情報記録装置において共通なマスターキーであることを特徴とする。

【００４２】さらに、本発明の情報記録方法の一実施態様において、前記暗号化キー生成用データは、特定の記録媒体に固有のメディアキーであることを特徴とする。

【００４３】さらに、本発明の情報記録方法の一実施態様において、前記ノードキーは更新可能なキーとして構成され、更新処理に際しては更新ノードキーを下位階層のノードキーまたはリーフキーの少なくともいずれかを含むキーにより暗号化したキー更新ブロック（ＫＲＢ）を更新対象となるリーフの情報記録装置に配布する構成であり、前記更新ステップは、前記キー更新ブロック（ＫＲＢ）の暗号処理により、前記更新ノードキーを取得する更新ノードキー取得ステップと、取得した更新ノードキーに基づいて前記暗号化キー生成用データの更新データを算出する更新データ取得ステップと、を含むことを特徴とする。

【００４４】さらに、本発明の情報記録方法の一実施態様において、前記暗号化キー生成用データは、更新情報としての世代番号が対応付けられた構成であり、前記暗号処理ステップは、さらに、前記記録媒体に対する暗号化データ格納時に、使用した前記暗号化キー生成用データの世代番号を記録時世代番号として前記記録媒体に格納するステップを含むことを特徴とする。

【００４５】さらに、本発明の情報記録方法の一実施態様において、前記暗号処理ステップは、第1の暗号化キー生成用データに基づいて前記記録媒体に対する格納データの第1の暗号化キーを生成して該第1の暗号化キーに基づく暗号化処理を前記格納データに対して実行するとともに、前記第1の暗号化キー生成用データを前記記録媒体に格納する再生機器制限なしのデータ暗号処理と、前記情報記録装置に内蔵した第２の暗号化キー生成用データに基づいて前記記録媒体に対する格納データの第２の暗号化キーを生成して該第２の暗号化キーに基づく暗号化処理を前記格納データに対して実行する再生機器制限ありのデータ暗号処理と、を選択的に実行することを特徴とする。

【００４６】さらに、本発明の情報記録方法の一実施態

様において、前記暗号処理ステップは、前記再生機器制限なしの暗号処理において、情報記録装置に格納された世代管理されたマスターキーと、記録媒体固有の記録媒体識別子であるディスクＩＤと、前記記録媒体に記録すべきデータ固有のタイトルキーと、情報記録装置の識別子であるデバイスＩＤとに基づいてタイトル固有キーを生成し、該タイトル固有キーに基づいて、前記第１の暗号化キーを生成し、前記再生機器制限ありの暗号処理において、情報記録装置に格納された世代管理されたマスターキーと、記録媒体固有の記録媒体識別子であるディスクＩＤと、前記記録媒体に記録すべきデータ固有のタイトルキーと、情報記録装置の固有キーであるデバイス固有キーとに基づいてタイトル固有キーを生成し、該タイトル固有キーに基づいて、前記第２の暗号化キーを生成する構成であることを特徴とする。

【００４７】さらに、本発明の情報記録方法の一実施態様において、間欠的なトランスポートパケットから成るトランスポートストリームを構成する各パケットに受信時刻情報（ＡＴＳ）を付加するトランスポート・ストリーム処理ステップを有し、前記暗号処理ステップは、前記受信時刻情報（ＡＴＳ）の付加された1以上のパケットからなるブロックデータに対する暗号化キーとしてブロックキーを生成し、前記記録媒体に対する格納データの暗号処理においては、前記暗号化キー生成用データと前記受信時刻情報（ＡＴＳ）を含むブロックデータ固有の付加情報であるブロックシードとを含むデータに基づいて暗号化キーとしてのブロックキーを生成することを特徴とする。

【００４８】さらに、本発明の情報記録方法の一実施態様において、前記暗号処理ステップは、前記記録媒体に対する格納データの暗号処理をＤＥＳアルゴリズムに従って実行することを特徴とする。

【００４９】さらに、本発明の情報記録方法の一実施態様において、データを構成するトランスポートストリームに含まれる各パケットに付加されたコピー制御情報を識別し、該コピー制御情報に基づいて記録媒体に対する記録実行の可否を制御することを特徴とする。

【００５０】さらに、本発明の情報記録方法の一実施態様において、コピーを制御するためのコピー制御情報としての２ビットのＥＭＩ(Encryption Mode Indicator)を識別し、該ＥＭＩに基づいて記録媒体に対する記録実行の可否を制御することを特徴とする。

【００５１】さらに、本発明の第４の側面は、記録媒体から情報を再生する情報再生方法であり、複数の異なる情報再生装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報再生装置固有のリーフキーの少なくともいずれかを用いて記録媒体に格納された暗号データの復号処理を実行する復号キーを生成するための復号キー生成用データの更新処理を実行する更新ステップと、前記更新ステップにおいて更新された復号キー生成用データに基づいて復号キーを生成して前記記録媒体に格納された暗号データの復号処理を実行する復号処理ステップと、を有することを特徴とする情報再生方法にある。

【００５２】さらに、本発明の情報再生方法の一実施態様において、前記復号キー生成用データは、複数の情報記録装置において共通なマスターキーであることを特徴とする。

【００５３】さらに、本発明の情報再生方法の一実施態様において、前記復号キー生成用データは、特定の記録媒体に固有のメディアキーであることを特徴とする。

【００５４】さらに、本発明の情報再生方法の一実施態様において、前記ノードキーは更新可能なキーとして構成され、更新処理に際しては更新ノードキーを下位階層のノードキーまたはリーフキーの少なくともいずれかを含むキーにより暗号化したキー更新ブロック（ＫＲＢ）を更新対象となるリーフの情報再生装置に配布する構成であり、前記更新ステップは、前記キー更新ブロック（ＫＲＢ）の暗号処理により、前記更新ノードキーを取得する更新ノードキー取得ステップと、取得した更新ノードキーに基づいて前記復号キー生成用データの更新データを算出する更新データ取得ステップと、を含むことを特徴とする。

【００５５】さらに、本発明の情報再生方法の一実施態様において、前記復号キー生成用データは、更新情報としての世代番号が対応付けられた構成であり、前記復号処理ステップは、前記記録媒体からの暗号化データの復号時に、該暗号化データの暗号処理時に使用した暗号化キー生成用データの世代番号を前記記録媒体から読み取り、該読み取られた世代番号に対応する復号キー生成用データを使用して復号キーを生成することを特徴とする。

【００５６】さらに、本発明の情報再生方法の一実施態様において、前記記録媒体に格納された第1の復号キー生成用データに基づいて前記記録媒体に格納された暗号データに対する第1の復号キーを生成して該第1の復号キーに基づく復号処理を前記暗号データに対して実行する再生機器制限なしのデータ復号処理と、前記情報記録装置に内蔵した第２の復号キー生成用データに基づいて前記記録媒体に格納された暗号データに対する第２の復号キーを生成して該第２の復号キーに基づく復号処理を前記暗号データに対して実行する再生機器制限ありのデータ復号処理と、を選択的に実行することを特徴とする。

【００５７】さらに、本発明の情報再生方法の一実施態様において、前記復号処理ステップは、前記再生機器制限なしの復号処理において、情報記録装置に格納された世代管理されたマスターキーを取得するとともに、記録媒体から、記録媒体固有の記録媒体識別子であるディスクＩＤと、復号対象データに固有のタイトルキーと、暗号データを記録した情報記録装置の識別子であるデバイ

ＳＩＤ情報記録装置の識別子であるデバイスＩＤとを取得し、前記マスターキー、ディスクＩＤ、タイトルキー、デバイスＩＤとに基づいてタイトル固有キーを生成し、該タイトル固有キーに基づいて、前記第１の復号キーを生成し、前記再生機器制限ありの復号処理において、情報記録装置に格納された世代管理されたマスターキーと、情報記録装置に格納された情報記録装置の固有キーであるデバイス固有キーとを取得するとともに、記録媒体から、記録媒体固有の記録媒体識別子であるディスクＩＤと、復号対象データに固有のタイトルキーとを取得し、前記マスターキー、ディスクＩＤ、タイトルキー、デバイス固有キーとに基づいてタイトル固有キーを生成し、該タイトル固有キーに基づいて、前記第２の復号キーを生成することを特徴とする。

【００５８】さらに、本発明の情報再生方法の一実施態様において、情報再生装置は、復号されたブロックデータを構成する複数のトランスポートパケットの各々に付加された受信時刻情報（ＡＴＳ）に基づいてデータ出力制御を実行するトランスポート・ストリーム処理手段を有し、前記復号処理ステップは、前記受信時刻情報（ＡＴＳ）の付加された1以上のパケットからなるブロックデータに対する復号キーとしてブロックキーを生成し、前記記録媒体に格納された暗号データの復号処理においては、前記復号キー生成用データと前記受信時刻情報（ＡＴＳ）を含むブロックデータ固有の付加情報であるブロックシードとを含むデータに基づいて復号キーとしてのブロックキーを生成することを特徴とする。

【００５９】さらに、本発明の情報再生方法の一実施態様において、前記復号処理ステップは、前記記録媒体に格納された暗号データの復号処理をＤＥＳアルゴリズムに従って実行することを特徴とする。

【００６０】さらに、本発明の情報再生方法の一実施態様において、データを構成するトランスポートストリームに含まれる各パケットに付加されたコピー制御情報を識別し、該コピー制御情報に基づいて記録媒体に格納されたデータの再生実行の可否を制御することを特徴とする。

【００６１】さらに、本発明の情報再生方法の一実施態様において、コピーを制御するためのコピー制御情報としての２ビットのＥＭＩ(Encryption Mode Indicator)を識別し、該ＥＭＩに基づいて記録媒体に格納されたデータの再生実行の可否を制御することを特徴とする。

【００６２】さらに、本発明の第５の側面は、情報を記録可能な情報記録媒体であって、複数の異なる情報記録装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報記録装置固有のリーフキーに含まれる更新ノードキーを下位階層のノードキーまたはリーフキーの少なくともいずれかを含むキーにより暗号化したキー更新ブロック（ＫＲＢ）を格納したことを特徴とする情報記録媒体にある。

【００６３】さらに、本発明の情報記録媒体の一実施態様において、情報記録装置において記録媒体に格納するデータの暗号化処理に用いる暗号化キーを生成するための暗号化キー生成用データを前記更新ノードキーによって暗号化したデータを含むことを特徴とする。

【００６４】さらに、本発明の情報記録媒体の一実施態様において、情報再生装置において記録媒体に格納された暗号データの復号処理に用いる復号キーを生成するための復号キー生成用データを前記更新ノードキーによって暗号化したデータを含むことを特徴とする。

【００６５】さらに、本発明の情報記録媒体の一実施態様において、暗号化キー生成用データまたは復号キー生成用データに関する世代情報を格納した構成であることを特徴とする。

【００６６】さらに、本発明の第６の側面は、情報記録媒体を製造する記録媒体製造装置であり、複数の異なる情報記録装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報記録装置固有のリーフキーに含まれる更新ノードキーを下位階層のノードキーまたはリーフキーの少なくともいずれかを含むキーにより暗号化したキー更新ブロック（ＫＲＢ）を格納するメモリと、前記メモリに格納されたキー更新ブロック（ＫＲＢ）の前記記録媒体に対する書き込み制御を実行する制御部と、を有することを特徴とする記録媒体製造装置にある。

【００６７】さらに、本発明の記録媒体製造装置の一実施態様において、前記メモリには、さらに、記録媒体識別子と、暗号化された暗号化キー生成用データまたは暗号化された復号キー生成用データの少なくともいずれかを格納し、前記制御部は、前記記録媒体識別子、暗号化された暗号化キー生成用データ、または暗号化された復号キー生成用データの少なくともいずれかについて、前記記録媒体に対する書き込み制御を実行する構成であることを特徴とする。

【００６８】さらに、本発明の記録媒体製造装置の一実施態様において、前記メモリには、さらに、暗号化キー生成用データまたは復号キー生成用データに関する世代情報を格納し、前記制御部は、前記世代情報の前記記録媒体に対する書き込み制御を実行する構成であることを特徴とする。

【００６９】さらに、本発明の第７の側面は、記録媒体を製造する記録媒体製造方法であり、複数の異なる情報記録装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報記録装置固有のリーフキーに含まれる更新ノードキーを下位階層のノードキーまたはリーフキーの少なくともいずれかを含むキーにより暗号化したキー更新ブロック（ＫＲＢ）をメモリに格納するステップと、前記メモリに格納されたキー更新ブロック（ＫＲＢ）の前記記録媒体に対する書き込みを実行するステップと、を有することを特徴とする記録媒体

製造方法にある。

【００７０】さらに、本発明の記録媒体製造方法の一実施態様において、前記メモリに、さらに、記録媒体識別子、暗号化された暗号化キー生成用データ、または暗号化された復号キー生成用データの少なくともいずれかを格納し、前記記録媒体識別子、暗号化された暗号化キー生成用データ、または暗号化された復号キー生成用データの少なくともいずれかについて、前記記録媒体に対する書き込みを実行することを特徴とする。

【００７１】さらに、本発明の記録媒体製造方法の一実施態様において、前記記録媒体製造方法において、前記メモリに、さらに、暗号化キー生成用データまたは復号キー生成用データに関する世代情報を格納し、前記制御部は、前記世代情報の前記記録媒体に対する書き込みを実行することを特徴とする。

【００７２】さらに、本発明の第８の側面は、記録媒体に情報を記録する情報記録処理をコンピュータ・システム上で実行せしめるコンピュータ・プログラムを提供するプログラム提供媒体であって、前記コンピュータ・プログラムは、複数の異なる情報記録装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報記録装置固有のリーフキーの少なくともいずれかを用いて記録媒体に対する格納データの暗号化処理を実行する暗号化キーを生成するための暗号化キー生成用データの更新処理を実行する更新ステップと、前記更新ステップにおいて更新された暗号化キー生成用データに基づいて暗号化キーを生成して前記記録媒体に格納するデータの暗号処理を実行する暗号処理ステップと、を有することを特徴とするプログラム提供媒体にある。

【００７３】さらに、本発明の第９の側面は、記録媒体に格納された情報を再生する情報再生処理をコンピュータ・システム上で実行せしめるコンピュータ・プログラムを提供するプログラム提供媒体であって、前記コンピュータ・プログラムは、複数の異なる情報再生装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報再生装置固有のリーフキーの少なくともいずれかを用いて記録媒体に格納された暗号データの復号処理を実行する復号キーを生成するための復号キー生成用データの更新処理を実行する更新ステップと、前記更新ステップにおいて更新された復号キー生成用データに基づいて復号キーを生成して前記記録媒体に格納された暗号データの復号処理を実行する復号処理ステップと、を有することを特徴とするプログラム提供媒体にある。

【００７４】

【作用】本発明の構成においては、ツリー（木）構造の階層的鍵配信方式を用いることにより、キー更新に必要な配信メッセージ量を小さく抑えている。すなわち、各機器をｎ分木の各葉（リーフ）に配置した構成の鍵配信方法を用い、記録媒体もしくは通信回線を介して、コンテンツデータの記録媒体への記録もしくは記録媒体からの再生に必要な鍵（マスターキーもしくはメディアキー）を配信し、これを用いて各装置がコンテンツデータの記録、再生を行う。

【００７５】また、本発明の１つの態様としては、記録媒体に記録するコンテンツの形式をＭＰＥＧ２ ＴＳパケット（ｐａｃｋｅｔ）とし、このパケットを記録装置が受信した時刻情報であるＡＴＳを付加して記録する。ＡＴＳは２４乃至３２ビットのデータであり、ある程度のランダム性がある。ここで、ＡＴＳはArrival TimeStamp（着信時刻スタンプ）の略である。記録媒体のひとつのブロック（セクタ）には、ＡＴＳを付加したＴＳパケットをＸ個記録することにし、その第１番目のＴＳパケットに付加されたＡＴＳを用いてそのブロックのデータを暗号化するブロックキーを生成する。

【００７６】このようにすることにより、各ブロックごとに固有の鍵を用いて暗号化することができ、また鍵を格納する特別な領域も不要となり、記録、再生時にメインデータ部以外のデータをアクセスする必要もなくなる。

【００７７】さらに、ＴＳパケットにＡＴＳだけでなくコピー制限情報(ＣＣＩ：Copy Control Information)も付加して記録し、ＡＴＳとＣＣＩを用いてブロックキーを生成するようにすることも可能である。

【００７８】なお、本発明の第８および第９の側面に係るプログラム提供媒体は、例えば、様々なプログラム・コードを実行可能な汎用コンピュータ・システムに対して、コンピュータ・プログラムをコンピュータ可読な形式で提供する媒体である。媒体は、ＣＤやＦＤ、ＭＯなどの記録媒体、あるいは、ネットワークなどの伝送媒体など、その形態は特に限定されない。

【００７９】このようなプログラム提供媒体は、コンピュータ・システム上で所定のコンピュータ・プログラムの機能を実現するための、コンピュータ・プログラムと提供媒体との構造上又は機能上の協働的関係を定義したものである。換言すれば、該提供媒体を介してコンピュータ・プログラムをコンピュータ・システムにインストールすることによって、コンピュータ・システム上では協働的作用が発揮され、本発明の他の側面と同様の作用効果を得ることができるのである。

【００８０】本発明のさらに他の目的、特徴や利点は、後述する本発明の実施例や添付する図面に基づくより詳細な説明によって明らかになるであろう。

【００８１】

【発明の実施の形態】［システム構成］図１は、本発明を適用した記録再生装置１００の一実施例構成を示すブロック図である。記録再生装置１００は、入出力Ｉ／Ｆ(Interface)１２０、ＭＰＥＧ(Moving Picture Experts Group)コーデック１３０、Ａ／Ｄ，Ｄ／Ａコンバータ１４１を備えた入出力Ｉ／Ｆ(Interface)１４０、暗号

処理手段１５０、ＲＯＭ（Read Only Memory）１６０、ＣＰＵ(Central Processing Unit)１７０、メモリ１８０、記録媒体１９５のドライブ１９０、さらにトランスポート・ストリーム処理手段（ＴＳ処理手段）３００を有し、これらはバス１１０によって相互に接続されている。

【００８２】入出力Ｉ／Ｆ１２０は、外部から供給される画像、音声、プログラム等の各種コンテンツを構成するディジタル信号を受信し、バス１１０上に出力するとともに、バス１１０上のディジタル信号を受信し、外部に出力する。ＭＰＥＧコーデック１３０は、バス１１０を介して供給されるＭＰＥＧ符号化されたデータを、ＭＰＥＧデコードし、入出力Ｉ／Ｆ１４０に出力するとともに、入出力Ｉ／Ｆ１４０から供給されるディジタル信号をＭＰＥＧエンコードしてバス１１０上に出力する。入出力Ｉ／Ｆ１４０は、Ａ／Ｄ，Ｄ／Ａコンバータ１４１を内蔵している。入出力Ｉ／Ｆ１４０は、外部から供給されるコンテンツとしてのアナログ信号を受信し、Ａ／Ｄ，Ｄ／Ａコンバータ１４１でＡ／Ｄ(Analog Digital)変換することで、ディジタル信号として、ＭＰＥＧコーデック１３０に出力するとともに、ＭＰＥＧコーデック１３０からのディジタル信号を、Ａ／Ｄ，Ｄ／Ａコンバータ１４１でＤ／Ａ(Digital Analog)変換することで、アナログ信号として、外部に出力する。

【００８３】暗号処理手段１５０は、例えば、１チップのＬＳＩ(Large Scale IntegratedCurcuit)で構成され、バス１１０を介して供給されるコンテンツとしてのディジタル信号を暗号化し、または復号し、バス１１０上に出力する構成を持つ。なお、暗号処理手段１５０は１チップＬＳＩに限らず、各種のソフトウェアまたはハードウェアを組み合わせた構成によって実現することも可能である。ソフトウェア構成による処理手段としての構成については後段で説明する。

【００８４】ＲＯＭ１６０は、例えば、記録再生装置ごとに固有の、あるいは複数の記録再生装置のグループごとに固有のデバイスキーであるリーフキーと、複数の記録再生装置、あるいは複数のグループに共有のデバイスキーであるノードキーを記憶している。ＣＰＵ１７０は、メモリ１８０に記憶されたプログラムを実行することで、ＭＰＥＧコーデック１３０や暗号処理手段１５０等を制御する。メモリ１８０は、例えば、不揮発性メモリで、ＣＰＵ１７０が実行するプログラムや、ＣＰＵ１７０の動作上必要なデータを記憶する。ドライブ１９０は、デジタルデータを記録再生可能な記録媒体１９５を駆動することにより、記録媒体１９５からディジタルデータを読み出し（再生し）、バス１１０上に出力するとともに、バス１１０を介して供給されるディジタルデータを、記録媒体１９５に供給して記録させる。また、プログラムをＲＯＭ１６０に、デバイスキーをメモリ１８０に記録する構成としてもよい。

【００８５】記録媒体１９５は、例えば、ＤＶＤ、ＣＤ等の光ディスク、光磁気ディスク、磁気ディスク、磁気テープ、あるいはＲＡＭ等の半導体メモリ等のディジタルデータの記憶可能な媒体であり、本実施の形態では、ドライブ１９０に対して着脱可能な構成であるとする。但し、記録媒体１９５は、記録再生装置１００に内蔵する構成としてもよい。

【００８６】トランスポート・ストリーム処理手段（ＴＳ処理手段）３００は、後段において図６以下を用いて詳細に説明するが、例えば複数のＴＶプログラム（コンテンツ）が多重化されたトランスポートストリームから特定のプログラム（コンテンツ）に対応するトランスポートパケットを取り出して、取り出したトランスポートストリームの出現タイミング情報を各パケットとともに記録媒体１９５に格納するためのデータ処理および、記録媒体１９５からの再生処理時の出現タイミング制御処理を行なう。

【００８７】トランスポートストリームには、各トランスポートパケットの出現タイミング情報としてのＡＴＳ（Arrival Time Stamp：着信時刻スタンプ）が設定されており、このタイミングはＭＰＥＧ２システムズで規定されている仮想的なデコーダであるＴ－ＳＴＤ(Transport stream System Target Decoder)を破綻させないように符号化時に決定され、トランスポートストリームの再生時には、各トランスポートパケットに付加されたＡＴＳによって出現タイミングを制御する。トランスポート・ストリーム処理手段（ＴＳ処理手段）３００は、これらの制御を実行する。例えば、トランスポートパケットを記録媒体に記録する場合には、各パケットの間隔を詰めたソースパケットとして記録するが、各トランスポートパケットの出現タイミングを併せて記録媒体に保存することにより、再生時に各パケットの出力タイミングを制御することが可能となる。トランスポート・ストリーム処理手段（ＴＳ処理手段）３００は、ＤＶＤ等の記録媒体１９５へのデータ記録時に、各トランスポートパケットの入力タイミングを表すＡＴＳ（ArrivalTime Stamp：着信時刻スタンプ）を付加して記録する。

【００８８】本発明の記録再生装置１００は、上述のＡＴＳの付加されたトランスポートストリームによって構成されるコンテンツについて、暗号処理手段１５０において暗号化処理を実行し、暗号化処理のなされたコンテンツを記録媒体１９５に格納する。さらに、暗号処理手段１５０は、記録媒体１９５に格納された暗号化コンテンツの復号処理を実行する。これらの処理の詳細については、後段で説明する。

【００８９】なお、図１に示す暗号処理手段１５０、ＴＳ処理手段３００は、理解を容易にするため、別ブロックとして示してあるが、両機能を実行する１つのワンチップＬＳＩとして構成してもよく、また、両機能をソフトウェアまたはハードウェアを組み合わせた構成によっ

て実現する構成としてもよい。

【００９０】本発明の記録再生装置の構成例としては図１に示す構成の他に図２に示す構成が可能である。図２に示す記録再生装置２００では、記録媒体２０５はドライブ装置としての記録媒体インタフェース（Ｉ／Ｆ）２１０から着脱が可能であり、この記録媒体２０５を別の記録再生装置に装着してもデータの読出し、書きこみが可能な構成としたものである。

【００９１】［データ記録処理およびデータ再生処理］次に、図１あるいは図２の記録再生装置における記録媒体に対するデータ記録処理および記録媒体からのデータ再生処理について、図３および図４のフローチャートを参照して説明する。外部からのディジタル信号のコンテンツを、記録媒体１９５に記録する場合においては、図３（Ａ）のフローチャートにしたがった記録処理が行われる。即ち、ディジタル信号のコンテンツ（ディジタルコンテンツ）が、例えば、IEEE(Institute of Electrical and Electronics Engineers)1394シリアルバス等を介して、入出力Ｉ／Ｆ１２０に供給されると、ステップＳ３０１において、入出力Ｉ／Ｆ１２０は、供給されるディジタルコンテンツを受信し、バス１１０を介して、ＴＳ処理手段３００に出力する。

【００９２】ＴＳ処理手段３００は、ステップＳ３０２において、トランスポートストリームを構成する各トランスポートパケットにＡＴＳを付加したブロックデータを生成して、バス１１０を介して、暗号処理手段１５０に出力する。

【００９３】暗号処理手段１５０は、ステップＳ３０３において、受信したディジタルコンテンツに対する暗号化処理を実行し、その結果得られる暗号化コンテンツを、バス１１０を介して、ドライブ１９０、あるいは記録媒体Ｉ／Ｆ２１０に出力する。暗号化コンテンツは、ドライブ１９０、あるいは記録媒体Ｉ／Ｆ２１０を介して記録媒体１９５に記録（Ｓ３０４）され、記録処理を終了する。なお、暗号処理手段１５０における暗号処理については後段で説明する。

【００９４】なお、IEEE1394シリアルバスを介して接続した装置相互間で、ディジタルコンテンツを伝送するときの、ディジタルコンテンツを保護するための規格として、本特許出願人であるソニー株式会社を含む５社によって、５ＣＤＴＣＰ(Five Company Digital Transmission Content Protection)（以下、適宜、ＤＴＣＰという）が定められているが、このＤＴＣＰでは、コピーフリーでないディジタルコンテンツを装置相互間で伝送する場合、データ伝送に先立って、送信側と受信側が、コピーを制御するためのコピー制御情報を正しく取り扱えるかどうかの認証を相互に行い、その後、送信側において、ディジタルコンテンツを暗号化して伝送し、受信側において、その暗号化されたディジタルコンテンツ（暗号化コンテンツ）を復号するようになっている。

【００９５】このＤＴＣＰに規格に基づくデータ送受信においては、データ受信側の入出力Ｉ／Ｆ１２０は、ステップＳ３０１で、IEEE1394シリアルバスを介して暗号化コンテンツを受信し、その暗号化コンテンツを、ＤＴＣＰに規格に準拠して復号し、平文のコンテンツとして、その後、暗号処理手段１５０に出力する。

【００９６】ＤＴＣＰによるディジタルコンテンツの暗号化は、時間変化するキーを生成し、そのキーを用いて行われる。暗号化されたディジタルコンテンツは、その暗号化に用いたキーを含めて、IEEE1394シリアルバス上を伝送され、受信側では、暗号化されたディジタルコンテンツを、そこに含まれるキーを用いて復号する。

【００９７】なお、ＤＴＣＰによれば、正確には、キーの初期値と、ディジタルコンテンツの暗号化に用いるキーの変更タイミングを表すフラグとが、暗号化コンテンツに含められる。そして、受信側では、その暗号化コンテンツに含まれるキーの初期値を、やはり、その暗号化コンテンツに含まれるフラグのタイミングで変更していくことで、暗号化に用いられたキーが生成され、暗号化コンテンツが復号される。但し、ここでは、暗号化コンテンツに、その復号を行うためのキーが含まれていると等価であると考えても差し支えないため、以下では、そのように考えるものとする。ここで、ＤＴＣＰについては、例えば、http://www.dtcp.comのURL(Uniform Resource Locator)で特定されるＷｅｂページにおいて、インフォメイショナルバージョン(Informational Version)の取得が可能である。

【００９８】次に、外部からのアナログ信号のコンテンツを、記録媒体１９５に記録する場合の処理について、図３（Ｂ）のフローチャートに従って説明する。アナログ信号のコンテンツ（アナログコンテンツ）が、入出力Ｉ／Ｆ１４０に供給されると、入出力Ｉ／Ｆ１４０は、ステップＳ３２１において、そのアナログコンテンツを受信し、ステップＳ３２２に進み、内蔵するＡ／Ｄ，Ｄ／Ａコンバータ１４１でＡ／Ｄ変換して、ディジタル信号のコンテンツ（ディジタルコンテンツ）とする。

【００９９】このディジタルコンテンツは、ＭＰＥＧコーデック１３０に供給され、ステップＳ３２３において、ＭＰＥＧエンコード、すなわちＭＰＥＧ圧縮による符号化処理が実行され、バス１１０を介して、暗号処理手段１５０に供給される。

【０１００】以下、ステップＳＳ３２４、Ｓ３２５、Ｓ３２６において、図３（Ａ）のステップＳ３０２、Ｓ３０３における処理と同様の処理が行われる。すなわち、ＴＳ処理手段３００によるトランスポートパケットに対するＡＴＳ付加、暗号処理手段１５０における暗号化処理が実行され、その結果得られる暗号化コンテンツを、記録媒体１９５に記録して、記録処理を終了する。

【０１０１】次に、記録媒体１９５に記録されたコンテンツを再生して、ディジタルコンテンツ、あるいはアナ

ログコンテンツとして出力する処理について図４のフローに従って説明する。ディジタルコンテンツとして外部に出力する処理は図４（Ａ）のフローチャートにしたがった再生処理として実行される。即ち、まず最初に、ステップＳ４０１において、ドライブ１９０または記録媒体Ｉ／Ｆ２１０によって、記録媒体１９５に記録された暗号化コンテンツが読み出され、バス１１０を介して、暗号処理手段１５０に出力される。

【０１０２】暗号処理手段１５０では、ステップＳ４０２において、ドライブ１９０または記録媒体Ｉ／Ｆ２１０から供給される暗号化コンテンツが復号処理され、復号データがバス１１０を介して、ＴＳ処理手段３００に出力される。

【０１０３】ＴＳ処理手段３００は、ステップＳ４０３において、トランスポートストリームを構成する各トランスポートパケットのＡＴＳから出力タイミングを判定し、ＡＴＳに応じた制御を実行して、バス１１０を介して、入出力Ｉ／Ｆ１２０に供給する。入出力Ｉ／Ｆ１２０は、ＴＳ処理手段３００からのディジタルコンテンツを、外部に出力し、再生処理を終了する。なお、ＴＳ処理手段３００の処理、暗号処理手段１５０におけるディジタルコンテンツの復号処理については後述する。

【０１０４】なお、入出力Ｉ／Ｆ１２０は、ステップＳ４０４で、IEEE1394シリアルバスを介してディジタルコンテンツを出力する場合には、ＤＴＣＰの規格に準拠して、上述したように、相手の装置との間で認証を相互に行い、その後、ディジタルコンテンツを暗号化して伝送する。

【０１０５】記録媒体１９５に記録されたコンテンツを再生して、アナログコンテンツとして外部に出力する場合においては、図４（Ｂ）のフローチャートに従った再生処理が行われる。

【０１０６】即ち、ステップＳ４２１、Ｓ４２２、Ｓ４２３において、図４（Ａ）のステップＳ４０１、Ｓ４０２、Ｓ４０３における場合とそれぞれ同様の処理が行われ、これにより、暗号処理手段１５０において得られた復号されたディジタルコンテンツは、バス１１０を介して、ＭＰＥＧコーデック１３０に供給される。

【０１０７】ＭＰＥＧコーデック１３０では、ステップＳ４２４において、ディジタルコンテンツがＭＰＥＧデコード、すなわち伸長処理が実行され、入出力Ｉ／Ｆ１４０に供給される。入出力Ｉ／Ｆ１４０は、ステップＳ４２４において、ＭＰＥＧコーデック１３０でＭＰＥＧデコードされたディジタルコンテンツを、内蔵するＡ／Ｄ，Ｄ／Ａコンバータ１４１でＤ／Ａ変換（Ｓ４２５）して、アナログコンテンツとする。そして、ステップＳ４２６に進み、入出力Ｉ／Ｆ１４０は、そのアナログコンテンツを、外部に出力し、再生処理を終了する。

【０１０８】［データフォーマット］次に、図５を用いて、本発明における記録媒体上のデータフォーマットを説明する。本発明における記録媒体上のデータの読み書きの最小単位をブロック(block)という名前で呼ぶ。１ブロックは、１９２＊Ｘ（エックス）バイト（例えばＸ＝３２）の大きさとなっている。

【０１０９】本発明では、ＭＰＥＧ２のＴＳ（トランスポート・ストリーム）パケット（１８８バイト）にＡＴＳを付加して１９２バイトとして、それをＸ個集めて１ブロックのデータとしている。ＡＴＳは２４乃至３２ビットの着信時刻を示すデータであり、先にも説明したようにArrival Time Stamp（着信時刻スタンプ）の略である。ＡＴＳは各パケットの着信時刻に応じたランダム性のあるデータとして構成される。記録媒体のひとつのブロック（セクタ）には、ＡＴＳを付加したＴＳ（トランスポート・ストリーム）パケットをＸ個記録する。本発明の構成では、トランスポートストリームを構成する各ブロックの第１番目のＴＳパケットに付加されたＡＴＳを用いてそのブロック（セクタ）のデータを暗号化するブロックキーを生成する。

【０１１０】ランダム性のあるＡＴＳを用いて暗号化用のブロックキーを生成することにより、ブロック毎に異なる固有キーが生成される。生成されたブロック固有キーを用いてブロック毎の暗号化処理を実行する。また、ＡＴＳを用いてブロックキーを生成する構成とすることにより、各ブロック毎の暗号化鍵を格納するための記録媒体上の領域が不要となり、メインデータ領域が有効に使用可能となる。さらに、データの記録、再生時にメインデータ部以外のデータをアクセスする必要もなくなり、処理が効率的になる。

【０１１１】なお、図５に示すブロック・シード（Block Seed）は、ＡＴＳを含む付加情報である。ブロック・シードは、さらにＡＴＳだけでなくコピー制限情報(ＣＣＩ：Copy Control Information)も付加した構成としてもよい。この場合、ＡＴＳとＣＣＩを用いてブロックキーを生成する構成とすることができる。

【０１１２】なお、本発明の構成においては、ＤＶＤ等の記録媒体上にデータを格納する場合、コンテンツの大部分のデータは暗号化されるが、図５の最下段に示すように、ブロックの先頭のｍ（たとえば、ｍ＝８または１６）バイトは暗号化されずに平文（Unencrypted data）のまま記録され、残りのデータ（ｍ＋１バイト以降）が暗号化される。これは暗号処理が８バイト単位としての処理であるために暗号処理データ長（Encrypted data）に制約が発生するためである。なお、もし、暗号処理が８バイト単位でなく、たとえば１バイト単位で行なえるなら、ｍ＝４として、ブロックシード以外の部分をすべて暗号化してもよい。

【０１１３】［ＴＳ処理手段における処理］ここで、ＡＴＳの機能について詳細に説明する。ＡＴＳは、先にも説明したように入力トランスポートストリーム中の各トランスポートパケットの出現タイミングを保存するため

に付加する着信時刻スタンプである。

【０１１４】すなわち、例えば複数のＴＶプログラム（コンテンツ）が多重化されたトランスポートストリームの中から１つまたは幾つかのＴＶプログラム（コンテンツ）を取り出した時、その取り出したトランスポートストリームを構成するトランスポートパケットは、不規則な間隔で現れる（図７（ａ）参照）。トランスポートストリームは、各トランスポートパケットの出現タイミングに重要な意味があり、このタイミングはＭＰＥＧ２システムズ(ISO/IEC 13818-1)で規定されている仮想的なデコーダであるＴ－ＳＴＤ(Transport stream System Target Decoder)を破綻させないように符号化時に決定される。

【０１１５】トランスポートストリームの再生時には、各トランスポートパケットに付加されたＡＴＳによって出現タイミングが制御される。従って、記録媒体にトランスポートパケットを記録する場合には、トランスポートパケットの入力タイミングを保存する必要があり、トランスポートパケットをＤＶＤ等の記録媒体に記録する時に、各トランスポートパケットの入力タイミングを表すＡＴＳを付加して記録する。

【０１１６】図６に、ディジタルインタフェース経由で入力されるトランスポートストリームをＤＶＤ等の記録媒体であるストレージメディアに記録する時のＴＳ処理手段３００において実行する処理を説明するブロック図を示す。端子６００からは、ディジタル放送等のディジタルデータとしてトランスポートストリームが入力される。図１または図２においては、入出力Ｉ／Ｆ１２０を介して、あるいは入出力Ｉ／Ｆ１４０、ＭＰＥＧコーデック１３０を介して端子６００からトランスポートストリームが入力される。

【０１１７】トランスポートストリームは、ビットストリームパーサー(parser)６０２に入力される。ビットストリームパーサー６０２は、入力トランスポートストリームの中からＰＣＲ(Program Clock Reference)パケットを検出する。ここで、ＰＣＲパケットとは、ＭＰＥＧ２システムズで規定されているＰＣＲが符号化されているパケットである。ＰＣＲパケットは、１００ｍｓｅｃ以内の時間間隔で符号化されている。ＰＣＲは、トランスポートパケットが受信側に到着する時刻を２７ＭＨｚの精度で表す。

【０１１８】そして、２７ＭＨｚＰＬＬ６０３において、記録再生器が持つ２７ＭＨｚクロックをトランスポートストリームのＰＣＲにロック（Lock）させる。タイムスタンプ発生回路６０４は、２７ＭＨｚクロックのクロックのカウント値に基づいたタイムスタンプを発生する。そして、ブロック・シード（Block seed）付加回路６０５は、トランスポートパケットの第1バイト目がスムージングバッファ６０６へ入力される時のタイムスタンプをＡＴＳとして、そのトランスポートパケットに付加する。

【０１１９】ＡＴＳが付加されたトランスポートパケットは、スムージングバッファ６０６を通って、端子６０７から、暗号処理手段１５０に出力され、後段で説明する暗号処理が実行された後、ドライブ１９０（図１）、記録媒体Ｉ／Ｆ２１０（図２）を介してストレージメディアである記録媒体１９５に記録される。

【０１２０】図7は、入力トランスポートストリームが記録媒体に記録される時の処理の例を示す。図７（ａ）は、ある特定プログラム（コンテンツ）を構成するトランスポートパケットの入力を示す。ここで横軸は、ストリーム上の時刻を示す時間軸である。この例ではトランスポートパケットの入力は、図７（ａ）に示すように不規則なタイミングで現れる。

【０１２１】図７（ｂ）は、ブロック・シード（Block Seed）付加回路６０５の出力を示す。ブロック・シード（Block Seed）付加回路６０５は、トランスポートパケット毎に、そのパケットのストリーム上の時刻を示すＡＴＳを含むブロック・シード（Block Seed）を付加して、ソースパケットを出力する。図７（ｃ）は記録媒体に記録されたソースパケットを示す。ソースパケットは、図７（ｃ）に示すように間隔を詰めて記録媒体に記録される。このように間隔を詰めて記録することにより記録媒体の記録領域を有効に使用できる。

【０１２２】図８は、記録媒体１９５に記録されたトランスポートストリームを再生する場合のＴＳ処理手段３００の処理構成ブロック図を示している。端子８００からは、後段で説明する暗号処理手段において復号されたＡＴＳ付きのトランスポートパケットが、ブロック・シード（Block seed）分離回路８０１へ入力され、ＡＴＳとトランスポートパケットが分離される。タイミング発生回路８０４は、再生器が持つ２７ＭＨｚクロック８０５のクロックカウンター値に基づいた時間を計算する。

【０１２３】なお、再生の開始時において、一番最初のＡＴＳが初期値として、タイミング発生回路８０４にセットされる。比較器８０３は、ＡＴＳとタイミング発生回路８０４から入力される現在の時刻を比較する。そして、タイミング発生回路８０４が発生する時間とＡＴＳが等しくなった時、出力制御回路８０２は、そのトランスポートパケットをＭＰＥＧコーデック１３０またはディジタル入出力Ｉ／Ｆ１２０へ出力する。

【０１２４】図９は、入力ＡＶ信号を記録再生器１００のＭＰＥＧコーデック１３０においてＭＰＥＧエンコードして、さらにＴＳ処理手段３００においてトランスポートストリームを符号化する構成を示す。従って図９は、図１または、図２おけるＭＰＥＧコーデック１３０とＴＳ処理手段３００の両処理構成を併せて示すブロック図である。端子９０１からは、ビデオ信号が入力されており、それはＭＰＥＧビデオエンコーダ９０２へ入力される。

【０１２５】ＭＰＥＧビデオエンコーダ９０２は、入力ビデオ信号をＭＰＥＧビデオストリームに符号化し、それをバッファビデオストリームバッファ９０３へ出力する。また、ＭＰＥＧビデオエンコーダ９０２は、ＭＰＥＧビデオストリームについてのアクセスユニット情報を多重化スケジューラ９０８へ出力する。ビデオストリームのアクセスユニットとは、ピクチャであり、アクセスユニット情報とは、各ピクチャのピクチャタイプ，符号化ビット量，デコードタイムスタンプである。ここで、ピクチャタイプは、Ｉ／Ｐ／Ｂピクチャ（picture）の情報である。また、デコードタイムスタンプは、ＭＰＥＧ２システムズで規定されている情報である。

【０１２６】端子９０４からは、オーディオ信号が入力されており、それはＭＰＥＧオーディオエンコーダ９０５へ入力される。ＭＰＥＧオーディオエンコーダ９０５は、入力オーディオ信号をＭＰＥＧオーディオストリームに符号化し、それをバッファ９０６へ出力する。また、ＭＰＥＧオーディオエンコーダ９０５は、ＭＰＥＧオーディオストリームについてのアクセスユニット情報を多重化スケジューラ９０８へ出力する。オーディオストリームのアクセスユニットとは、オーディオフレームであり、アクセスユニット情報とは、各オーディオフレームの符号化ビット量，デコードタイムスタンプである。

【０１２７】多重化スケジューラ９０８には、ビデオとオーディオのアクセスユニット情報が入力される。多重化スケジューラ９０８は、アクセスユニット情報に基づいて、ビデオストリームとオーディオストリームをトランスポートパケットに符号化する方法を制御する。多重化スケジューラ９０８は、内部に２７ＭＨｚ精度の基準時刻を発生するクロックを持ち、そして、ＭＰＥＧ２で規定されている仮想的なデコーダモデルであるＴ－ＳＴＤを満たすようにして、トランスポートパケットのパケット符号化制御情報を決定する。パケット符号化制御情報は、パケット化するストリームの種類とストリームの長さである。

【０１２８】パケット符号化制御情報がビデオパケットの場合、スイッチ９７６はａ側になり、ビデオストリームバッファ９０３からパケット符号化制御情報により指示されたペイロードデータ長のビデオデータが読み出され、トランスポートパケット符号化器９０９へ入力される。

【０１２９】パケット符号化制御情報がオーディオパケットの場合、スイッチ９７６はｂ側になり、オーディオストリームバッファ９０６から指示されたペイロードデータ長のオーディオデータが読み出され、トランスポートパケット符号化器９０９へ入力される。

【０１３０】パケット符号化制御情報がＰＣＲパケットの場合、トランスポートパケット符号化器９０９は、多重化スケジューラ９０８から入力されるＰＣＲを取り込み、ＰＣＲパケットを出力する。パケット符号化制御情報がパケットを符号化しないことを指示する場合、トランスポートパケット符号化器９０９へは何も入力されない。

【０１３１】トランスポートパケット符号化器９０９は、パケット符号化制御情報がパケットを符号化しないことを指示する場合、トランスポートパケットを出力しない。それ以外の場合、パケット符号化制御情報に基づいてトランスポートパケットを生成し、出力する。したがって、トランスポートパケット符号化器９０９は、間欠的にトランスポートパケットを出力する。到着（Arrival）タイムスタンプ（time stamp）計算手段９１０は、多重化スケジューラ９０８から入力されるＰＣＲに基づいて、トランスポートパケットの第1バイト目が受信側に到着する時刻を示すＡＴＳを計算する。

【０１３２】多重化スケジューラ９０８から入力されるＰＣＲは、ＭＰＥＧ２で規定されるトランスポートパケットの１０バイト目の受信側への到着時刻を示すので、ＡＴＳの値は、ＰＣＲの時刻から１０バイト前のバイトが到着する時刻となる。

【０１３３】ブロック・シード（Block Seed）付加回路９１１は、トランスポートパケット符号化器９０９から出力されるトランスポートパケットにＡＴＳを付加する。ブロック・シード（Block seed）付加回路９１１から出力されるＡＴＳ付きのトランスポートパケットは、スムージングバッファ９１２を通って、暗号処理手段１５０へ入力され、後段で説明する暗号処理が実行された後、ストレージメディアである記録媒体１９５へ格納される。

【０１３４】記録媒体１９５へ格納されるＡＴＳ付きのトランスポートパケットは、暗号処理手段１５０で暗号化される前に図７（ｃ）に示すように間隔を詰めた状態で入力され、その後、記録媒体１９５に格納される。トランスポートパケットが間隔を詰めて記録されても、ＡＴＳを参照することによって、そのトランスポートパケットの受信側への入力時刻を制御することができる。

【０１３５】ところで、ＡＴＳの大きさは３２ビットに決まっているわけではなく、２４ビット乃至３１ビットでも構わない。ＡＴＳのビット長が長いほど、ＡＴＳの時間カウンターが一周する周期が長くなる。例えば、ＡＴＳが２７ＭＨｚ精度のバイナリーカウンターである場合、２４－ｂｉｔ長のＡＴＳが一周する時間は、約0.6秒である。この時間間隔は、一般のトランスポートストリームでは十分な大きさである。なぜなら、トランスポートストリームのパケット間隔は、ＭＰＥＧ２の規定により、最大０．１秒と決められているからである。しかしながら、十分な余裕を見て、ＡＴＳを２４－ｂｉｔ以上にしても良い。

【０１３６】このように、ＡＴＳのビット長を様々な長さとした場合、ブロックデータの付加データであるブロ

ックシードの構成としていくつかの構成が可能となる。ブロック・シードの構成例を図１０に示す。図１０の例１は、ＡＴＳを３２ビット分使用ずる例である。図１０の例２は、ＡＴＳを３０ビットとし、コピー制御情報（CCI）を２ビット分使用する例である。コピー制御情報は、それが付加されたデータのコピー制御の状態を表す情報であり、ＳＣＭＳ：Serial Copy Management SystemやＣＧＭＳ：Copy Generation Management Systemが有名である。これらのコピー制御情報では、その情報が付加されたデータは制限なくコピーが許可されていることを示すコピーフリー（Copy Free）、1世代のみのコピーを許可する1世代コピー許可（One Generation Copy Allowed）、コピーを認めないコピー禁止（Copy Prohibited）などの情報が表せる。

【０１３７】図１０に示す例3は、ＡＴＳを２４ビットとし、ＣＣＩを２ビット使用し、さらに他の情報を6ビット使用する例である。他の情報としては、たとえばこのデータがアナログ出力される際に、アナログ映像データのコピー制御機構であるマクロビジョン（Macrovision）のオン／オフ（On/Off）を示す情報など、様々な情報を利用することが可能である。

【０１３８】［キー配信構成としてのツリー（木）構造について］次に、図１または図２に示した記録再生装置が、データを記録媒体に記録、もしくは記録媒体から再生する際に必要なマスターキーを、各機器に配布する構成について説明する。図１１は、本方式を用いた記録システムにおける記録再生装置の鍵の配布構成を示した図である。図１１の最下段に示すナンバ０～１５が個々の記録再生装置である。すなわち図１１に示す木（ツリー）構造の各葉(リーフ：leaf)がそれぞれの記録再生装置に相当する。

【０１３９】各デバイス０～１５は、製造時（出荷時）に、あらかじめ定められている初期ツリーにおける、自分のリーフからルートに至るまでのノードに割り当てられた鍵（ノードキー）および各リーフのリーフキーを自身で格納する。図１１の最下段に示すＫ０００～Ｋ１１１１が各デバイス０～１５にそれぞれ割り当てられたリーフキーであり、最上段のＫＲから、最下段から２番目の節（ノード）に記載されたキー：ＫＲ～Ｋ１１１をノードキーとする。

【０１４０】図１１に示すツリー構成において、例えばデバイス０はリーフキーＫ０００００と、ノードキー：Ｋ０００、Ｋ００、Ｋ０、ＫＲを所有する。デバイス５はＫ０１０１、Ｋ０１０、Ｋ０１、Ｋ０、ＫＲを所有する。デバイス１５は、Ｋ１１１１、Ｋ１１１、Ｋ１１、Ｋ１、ＫＲを所有する。なお、図１１のツリーにはデバイスが０～１５の１６個のみ記載され、ツリー構造も４段構成の均衡のとれた左右対称構成として示しているが、さらに多くのデバイスがツリー中に構成され、また、ツリーの各部において異なる段数構成を持つことが可能である。

【０１４１】また、図１１のツリー構造に含まれる各記録再生器には、様々な記録媒体、例えばＤＶＤ、ＣＤ、ＭＤ、メモリスティック（商標）等を使用する様々なタイプの記録再生器が含まれている。さらに、様々なアプリケーションサービスが共存することが想定される。このような異なるデバイス、異なるアプリケーションの共存構成の上に図１１に示すキー配布構成が適用されている。

【０１４２】これらの様々なデバイス、アプリケーションが共存するシステムにおいて、例えば図１１の点線で囲んだ部分、すなわちデバイス０，１，２，３を同一の記録媒体を用いるひとつのグループとして設定する。例えば、この点線で囲んだグループ内に含まれるデバイスに対しては、まとめて、共通のコンテンツを暗号化してプロバイダから送付したり、共通に使用するマスターキーを送付したり、あるいは各デバイスからプロバイダあるいは決済機関等にコンテンツ料金の支払データをやはり暗号化して出力するといった処理が実行される。コンテンツプロバイダ、あるいは決済処理機関等、各デバイスとのデータ送受信を行なう機関は、図１１の点線で囲んだ部分、すなわちデバイス０，１，２，３を１つのグループとして一括してデータを送付する処理を実行する。このようなグループは、図１１のツリー中に複数存在する。

【０１４３】なお、ノードキー、リーフキーは、ある１つの鍵管理センタによって統括して管理してもよいし、各グループに対する様々なデータ送受信を行なうプロバイダ、決済機関等によってグループごとに管理する構成としてもよい。これらのノードキー、リーフキーは例えばキーの漏洩等の場合に更新処理が実行され、この更新処理は鍵管理センタ、プロバイダ、決済機関等が実行する。

【０１４４】このツリー構造において、図１１から明らかなように、１つのグループに含まれる３つのデバイス０，１，２，３はノードキーとして共通のキーＫ００、Ｋ０、ＫＲを保有する。このノードキー共有構成を利用することにより、例えば共通のマスターキーをデバイス０，１，２，３のみに提供することが可能となる。たとえば、共通に保有するノードキーＫ００自体をマスターキーとして設定すれば、新たな鍵送付を実行することなくデバイス０，１，２，３のみが共通のマスターキーの設定が可能である。また、新たなマスターキーKmasterをノードキーＫ００で暗号化した値Ｅｎｃ（Ｋ００，Kmaster）を、ネットワークを介してあるいは記録媒体に格納してデバイス０，１，２，３に配布すれば、デバイス０，１，２，３のみが、それぞれのデバイスにおいて保有する共有ノードキーＫ００を用いて暗号Ｅｎｃ（Ｋ００，Kmaster）を解いてマスターキー：Kmasterを得ることが可能となる。なお、Ｅｎｃ（Ｋａ，Ｋｂ）はＫ

ｂをＫａによって暗号化したデータであることを示す。

【０１４５】また、ある時点ｔにおいて、デバイス３の所有する鍵：Ｋ００１１，Ｋ００１，Ｋ００，Ｋ０，ＫＲが攻撃者（ハッカー）により解析されて露呈したことが発覚した場合、それ以降、システム（デバイス０，１，２，３のグループ）で送受信されるデータを守るために、デバイス３をシステムから切り離す必要がある。そのためには、ノードキー：Ｋ００１，Ｋ００，Ｋ０，ＫＲをそれぞれ新たな鍵Ｋ（ｔ）００１，Ｋ（ｔ）００，Ｋ（ｔ）０，Ｋ（ｔ）Ｒに更新し、デバイス０，１，２にその更新キーを伝える必要がある。ここで、Ｋ（ｔ）ａａａは、鍵Ｋａａａの世代（Generation）：ｔの更新キーであることを示す。

【０１４６】更新キーの配布処理ついて説明する。キーの更新は、例えば、図１２（Ａ）に示すキー更新ブロック（ＫＲＢ：Key Renewal Block）と呼ばれるブロックデータによって構成されるテーブルをたとえばネットワーク、あるいは記録媒体に格納してデバイス０，１，２に供給することによって実行される。

【０１４７】図１２（Ａ）に示すキー更新ブロック（ＫＲＢ）には、ノードキーの更新の必要なデバイスのみが更新可能なデータ構成を持つブロックデータとして構成される。図１２の例は、図１１に示すツリー構造中のデバイス０，１，２において、世代ｔの更新ノードキーを配布することを目的として形成されたブロックデータである。図１１から明らかなように、デバイス０，デバイス１は、更新ノードキーとしてＫ（ｔ）００、Ｋ（ｔ）０、Ｋ（ｔ）Ｒが必要であり、デバイス２は、更新ノードキーとしてＫ（ｔ）００１、Ｋ（ｔ）００、Ｋ（ｔ）０、Ｋ（ｔ）Ｒが必要である。

【０１４８】図１２（Ａ）のＫＲＢに示されるようにＫＲＢには複数の暗号化キーが含まれる。最下段の暗号化キーは、Ｅｎｃ（Ｋ００１０，Ｋ（ｔ）００１）である。これはデバイス２の持つリーフキーＫ００１０によって暗号化された更新ノードキーＫ（ｔ）００１であり、デバイス２は、自身の持つリーフキーによってこの暗号化キーを復号し、Ｋ（ｔ）００１を得ることができる。また、復号により得たＫ（ｔ）００１を用いて、図１２（Ａ）の下から２段目の暗号化キーＥｎｃ（Ｋ（ｔ）００１，Ｋ（ｔ）００）を復号可能となり、更新ノードキーＫ（ｔ）００を得ることができる。以下順次、図１２（Ａ）の上から２段目の暗号化キーＥｎｃ（Ｋ（ｔ）００，Ｋ（ｔ）０）を復号し、更新ノードキーＫ（ｔ）０、図１２（Ａ）の上から１段目の暗号化キーＥｎｃ（Ｋ（ｔ）０，Ｋ（ｔ）Ｒ）を復号しＫ（ｔ）Ｒを得る。一方、デバイス０，１は、ノードキーＫ００００は更新する対象に含まれておらず、更新ノードキーとして必要なのは、Ｋ（ｔ）００、Ｋ（ｔ）０、Ｋ（ｔ）Ｒである。デバイス０，１は、図１２（Ａ）の上から３段目の暗号化キーＥｎｃ（Ｋ０００，Ｋ（ｔ）００）を復号しＫ（ｔ）００を取得し、以下、図１２（Ａ）の上から２段目の暗号化キーＥｎｃ（Ｋ（ｔ）００，Ｋ（ｔ）０）を復号し、更新ノードキーＫ（ｔ）０、図１２（Ａ）の上から１段目の暗号化キーＥｎｃ（Ｋ（ｔ）０，Ｋ（ｔ）Ｒ）を復号しＫ（ｔ）Ｒを得る。このようにして、デバイス０，１，２は更新した鍵Ｋ（ｔ）００，Ｋ（ｔ）０，Ｋ（ｔ）Ｒを得ることができる。なお、図１２（Ａ）のインデックスは、復号キーとして使用するノードキー、リーフキーの絶対番地を示す。

【０１４９】図１１に示すツリー構造の上位段のノードキー：Ｋ０，ＫＲの更新が不要であり、ノードキーＫ００のみの更新処理が必要である場合には、図１２（Ｂ）のキー更新ブロック（ＫＲＢ：Key Renewal Block）を用いることで、更新ノードキーＫ（ｔ）００をデバイス０，１，２に配布することができる。

【０１５０】図１２（Ｂ）に示すＫＲＢは、例えば特定のグループにおいて共有する新たなマスターキーを配布する場合に利用可能である。具体例として、図１１に点線で示すグループ内のデバイス０，１，２，３がある記録媒体を用いており、新たな共通のマスターキーＫ（ｔ）masterが必要であるとする。このとき、デバイス０，１，２，３の共通のノードキーＫ００を更新したＫ（ｔ）００を用いて新たな共通の更新マスターキー：Ｋ（ｔ）masterを暗号化したデータＥｎｃ（Ｋ（ｔ），Ｋ（ｔ）master）を図１２（Ｂ）に示すＫＲＢとともに配布する。この配布により、デバイス４など、その他のグループの機器においては復号されないデータとしての配布が可能となる。

【０１５１】すなわち、デバイス０，１，２はＫＲＢを処理して得たＫ（ｔ）００を用いて上記暗号文を復号すれば、ｔ時点でのマスターキーＫ（ｔ）masterを得ることが可能になる。

【０１５２】［ＫＲＢを使用したマスターキーの配布］図１３に、ｔ時点でのマスターキーＫ（ｔ）masterを得る処理例として、Ｋ（ｔ）００を用いて新たな共通のマスターキーＫ（ｔ）masterを暗号化したデータＥｎｃ（Ｋ（ｔ）００，Ｋ（ｔ）master）と図１２（Ｂ）に示すＫＲＢとを記録媒体を介して受領したデバイス０の処理を示す。

【０１５３】図１３に示すように、デバイス０は、記録媒体に格納されている世代：ｔ時点のＫＲＢと自分があらかじめ格納しているノードキーＫ０００を用いて上述したと同様のＫＲＢ処理により、ノードキーＫ（ｔ）００を生成する。さらに、復号した更新ノードキーＫ（ｔ）００を用いて更新マスターキーＫ（ｔ）masterを復号して、後にそれを使用するために自分だけが持つリーフキーＫ０００００で暗号化して格納する。なお、デバイス０が更新マスターキーＫ（ｔ）master を安全に自身内に格納できる場合、リーフキーＫ０００００で暗号化する必要はない。

【０１５４】また、この更新マスターキーの取得処理を図１４のフローチャートにより説明する。なお、記録再生装置は出荷時にその時点で最新のマスターキー：Ｋ（ｃ）masterを与えられ、自身のメモリに安全に（具体的にはたとえば、自身のリーフキーで暗号化して）格納しているものとする。

【０１５５】更新マスターキーＫ（ｎ）masterとＫＲＢの格納された記録媒体が、記録再生装置にセットされると、まず最初に、ステップＳ１４０１において、記録再生装置は、記録媒体から、記録媒体に格納されているマスターキーＫ（ｎ）masterの時点（世代）番号：ｎ（これを、プレ（pre－recording）記録世代情報（Generation#n）と呼ぶことにする）を読み出す。記録媒体には、予め、マスターキーＫ（ｎ）masterの時点（世代）番号：ｎが記憶されている。また、自身が保持している暗号化マスターキーＣを読み出し、ステップＳ１４０２において、その暗号化マスターキーの世代：ｃと、プレ記録世代情報Generation#nが表す世代：ｎとを比較して、その世代の前後を判定する。

【０１５６】ステップＳ１４０２において、プレ記録世代情報Generation#nが表す世代：ｎの方が、自身のメモリに記憶された暗号化マスターキーＣの世代：ｃよりも後でない（新しくない）と判定された場合、即ち、メモリに記憶された暗号化マスターキーＣの世代：ｃが、プレ記録世代情報Generation#nが表す世代：ｎと同一か、または後の場合、ステップＳ１４０３乃至Ｓ１４０８をスキップして、マスターキー更新処理を終了する。即ち、この場合、自身のメモリに記憶されたマスターキーＫ（ｃ）master（暗号化マスターキーＣ）の更新は行う必要がないので、その更新は行われない。

【０１５７】一方、ステップＳ１４０２において、プレ記録世代情報Generation#nが表す世代：ｎの方が、メモリに記憶された暗号化マスターキーＣの世代：ｃよりも後である（新しい）と判定された場合、即ち、メモリに記憶された暗号化マスターキーＣの世代が、プレ記録世代情報Generation#nが表す世代ｎよりも前の世代である場合、ステップＳ１４０３に進み、記録再生装置は、記録媒体から、キー更新ブロック（ＫＲＢ：Key Renewal Block)を読み出す。

【０１５８】ステップＳ１４０４において、記録再生装置は、ステップＳ１４０３で読み出したＫＲＢと、自身がメモリに格納しているリーフキー（図１１のデバイス０におけるＫ００００）およびノードキー（図１１のデバイス０におけるＫ０００，Ｋ００...）を用いて、プレ記録世代情報Generation#n（図１３におけるｔ）時点でのノード００の鍵Ｋ（ｔ）００を計算する。

【０１５９】ステップＳ１４０５では、ステップＳ１４０４においてＫ（ｔ）００を得られたか否かを検査する。得られなかった場合は、その時点においてその記録再生装置がツリー構成のグループからリボーク（排除）されていることを示すので、ステップＳ１４０６乃至Ｓ１４０８をスキップしてマスターキー更新処理を終了する。

【０１６０】Ｋ（ｔ）００を得られた場合、ステップＳ１４０６に進み、記録媒体からＥｎｃ（Ｋ（ｔ）００，Ｋ（ｔ）master)、すなわち、Ｋ（ｔ）００を用いてｔ時点でのマスターキーを暗号化した値を読み出す。そしてステップＳ１４０７において、この暗号文をＫ（ｔ）００を用いて復号してＫ（ｔ）masterを計算する。

【０１６１】ステップＳ１４０８では、自身のみが持つリーフキー（図１１のデバイス０におけるＫ００００）を用いてＫ（ｔ）masterを暗号化してメモリに格納する。以上で、マスターキーの更新処理が完了する。

【０１６２】ところで、マスターキーは、時点（世代）０から昇順に使用されていくが、新しい世代のマスターキーから、古い世代のマスターキーを計算によりシステム内の各機器が求められる構成とすることが望ましい。すなわち、記録再生装置は、一方向性関数ｆを保持しており、その一方向性関数ｆに、自身が持つマスターキーを、そのマスターキーの世代と、必要なマスターキーの世代との差に対応する回数だけ適用することにより、調べた世代のマスターキーを作成する。

【０１６３】具体的には、例えば、記録再生装置に記憶されているマスターキーＭＫの世代が世代ｉ＋１であり、あるデータの再生に必要な（記録時に使用された）マスターキーＭＫの世代が世代ｉ－１である場合、マスターキーＫ（ｉ－１）masterは、記録再生装置において、一方向性関数ｆが２回用いられ、ｆ（ｆ（Ｋ（ｉ＋１）master））を計算することにより生成される。

【０１６４】また、記録再生装置に記憶されているマスターキーの世代が世代ｉ＋１であり、必要なマスターキーの世代が世代ｉ－２である場合、マスターキーＫ（ｉ－２）masterは、一方向性関数ｆを３回用いて、ｆ（ｆ（ｆ（Ｋ（ｉ＋１）master））)を計算することにより生成される。

【０１６５】ここで、一方向性関数としては、例えば、ハッシュ(hash)関数を用いることができる。具体的には、例えば、ＭＤ５(Message Digest 5)や、ＳＨＡ－１(Secure Hash Algorithm - 1)等を採用することができる。キーを発行するキー発行機関は、これらの一方向性関数を用いて自身の世代より前の世代を生成可能なマスターキーＫ（０）master，Ｋ（１）master，Ｋ（２）master・・・，Ｋ（Ｎ）masterを、あらかじめ求めておく。即ち、まず最初に、第Ｎ世代のマスターキーＫ（Ｎ）masterを設定し、そのマスターキーＫ（Ｎ）masterに、一方向性関数を１回ずつ適用しいくことで、それより前の世代のマスターキーＫ（Ｎ－１）master，Ｋ（Ｎ－２）master，・・・，Ｋ（１）master，Ｋ（０）masterを順次生成しておく。そして、世代の小さい（前の）マスターキーＫ（０）masterから順番に使用してい

く。なお、自身の世代より前の世代のマスターキーを生成するのに用いる一方向性関数は、すべての記録再生装置に設定されているものとする。

【０１６６】また、一方向性関数としては、例えば、公開鍵暗号技術を採用することも可能である。この場合、キー発行機関は、公開鍵暗号方式の秘密鍵を所有し、その秘密鍵に対する公開鍵を、すべての再生装置に与えておく。そして、キー発行機関は、第０世代のマスターキーＫ（０）masterを設定し、そのマスターキーＫ（０）masterから使用していく。即ち、キー発行機関は、第１世代以降のマスターキーＫ（ｉ）masterが必要になったら、その１世代前のマスターキーＫ（ｉ－１）masterを、秘密鍵で変換することにより生成して使用する。この場合、キー発行機関は、一方向性関数を用いて、Ｎ世代のマスターキーを、あらかじめ生成しておく必要がない。また、この方法によれば、理論上は、無制限の世代のマスターキーを生成することができる。なお、記録再生装置では、ある世代のマスターキーを有していれば、そのマスターキーを、公開鍵で変換することにより、その世代より前の世代のマスターキーを得ることができる。

【０１６７】次に、この記録再生装置がコンテンツを自身の記録媒体に記録する場合の、記録再生装置の処理について図１５のフローチャートを用いて説明する。コンテンツデータは、ある世代のマスターキーにより暗号化されてネットワークあるいは記録媒体を介してコンテンツプロバイタから各記録再生装置に配布される。

【０１６８】まず最初に、ステップＳ１５０１において、記録再生装置は、記録媒体から、プレ記録世代情報Generation#nを読み出す。また、自身のメモリが記憶している暗号化マスターキーＣの世代ｃを取得し、ステップＳ１５０２において、その暗号化マスターキーの世代ｃと、プレ記録世代情報Generation#nが表す世代ｎとを比較して、その世代の前後を判定する。

【０１６９】ステップＳ１５０２において、メモリに記憶された暗号化マスターキーＣの世代ｃが、プレ記録世代情報Generation#nが表す世代ｎ以後でないと判定された場合、即ち、メモリに記憶された暗号化マスターキーＣの世代ｃが、プレ記録世代情報Generation#nが表す世代ｎよりも古い世代である場合、ステップＳ１５０３をスキップして、すなわち、コンテンツデータの記録処理を行わずに終了する。

【０１７０】一方、ステップＳ１５０２において、自身の記録再生装置内のメモリに記憶された暗号化マスターキーＣの世代が、プレ記録世代情報Generation#nが表す世代ｎ以後であると判定された場合、即ち、メモリに記憶された暗号化マスターキーＣの世代が、プレ記録世代情報Generation#nが表す世代ｎと同一か、またはそれよりも新しい場合、ステップＳ１５０３に進み、コンテンツデータの記録処理を行う。

【０１７１】［世代管理のなされたマスターキーによるコンテンツデータ暗号化および記録処理］以下、世代管理のなされたマスターキーによってコンテンツデータの暗号化処理を実行して、自己の記録媒体に格納する処理について説明する。なお、ここでは、先に説明したトランスポートストリームによって構成されるデータを世代管理されたマスターキーを利用したデータに基づいてブロックキーを生成してブロックキーによりコンテンツデータを暗号化して記録媒体に格納する処理について説明する。また、記録再生装置が記録媒体に記録したデータを他の再生機器において再生可能とする設定と再生不可能とする設定が可能な構成を例として説明する。

【０１７２】図１６、図１７の処理ブロック図および図１８のフローチャートを用いて説明する。ここでは、記録媒体として光ディスクを例とする。この実施例では、記録媒体上のデータのbit-by-bitコピーを防ぐために、記録媒体固有の識別情報としてのディスクＩＤ(Disc ID)を、データを暗号化する鍵に作用させるようにしている。

【０１７３】図１６、図１７の処理ブロック図に従って、暗号処理手段１５０が実行するデータの暗号化処理の概要について説明する。

【０１７４】記録再生装置１６００は自身のメモリ１８０（図１，２参照）に格納しているマスターキー１６０１、デバイス識別子としてのデバイスＩＤ１６３１、デバイス固有キー１６３２を読み出す。マスターキー１６０１は、ライセンスを受けた記録再生装置に格納された秘密キーであり、前述のように世代管理がなされており、それぞれに世代番号が対応付けられている。このマスターキーは、複数の記録再生装置に共通なキー、例えば図１１に示す点線枠のグループに属するデバイスに共通なキーである。デバイスＩＤは記録再生装置１６００の識別子であり、予め記録再生装置に格納されている例えば製造番号等の識別子である。このデバイスＩＤは公開されていてもよい。デバイス固有キーは、その記録再生器１６００に固有の秘密鍵であり、予め個々の記録再生装置に応じて異なるように設定されて格納されたキーである。これらは予め記録再生装置１６００のメモリに格納されている。

【０１７５】記録再生装置１６００は例えば光ディスクである記録媒体１６２０に識別情報としてのディスクＩＤ（Disc ID）１６０３が既に記録されているかどうかを検査する。記録されていれば、ディスクＩＤ（Disc ID）１６０３を読出し（図１６に相当）、記録されていなければ、暗号処理手段１５０においてランダムに、もしくはあらかじめ定められた例えば乱数発生等の方法でディスクＩＤ（Disc ID）１７０１を生成し、ディスクに記録する（図１７に相当）。ディスクＩＤ（Disc ID）１６０３はそのディスクにひとつあればよいので、リードインエリアなどに格納することも可能である。

【０１７６】記録再生器１６００は、次にマスターキーとディスクＩＤを用いて、ディスク固有キー（Disc Unique Key）を生成１６０２する。ディスク固有キー（Disc Unique Key）の具体的な生成方法としては、図１９に示すように、ブロック暗号関数を用いたハッシュ関数にマスターキー（Master Key）とディスクＩＤ（Disc ID）を入力して得られた結果を用いる例１の方法や、FIPS 180-1で定められているハッシュ関数ＳＨＡ－１に、マスターキーとディスクＩＤ（Disc ID）とのビット連結により生成されるデータを入力し、その１６０ビットの出力から必要なデータ長のみをディスク固有キー（Disc Unique Key）として使用する例２の方法が適用できる。

【０１７７】次に、記録ごとの固有鍵であるタイトルキー（Title Key）を暗号処理手段１５０（図１，２，参照）においてランダムに、もしくはあらかじめ定められた例えば乱数発生等の方法で生成１６０４し、ディスク１６２０に記録する。

【０１７８】さらに、このタイトル（データ）がデータ記録を実行した記録再生装置でのみ再生可能とする（機器制限あり）か、他の機器においても再生可能とする（再生機器制限なし）のいずれであるかを示すフラグ、すなわち再生機器制限フラグ（Player Restriction Flag）を設定し１６３３、ディスク１６２０に記録する１６３５。さらに、機器識別情報としてのデバイスＩＤ取り出して１６３１、ディスク１６２０に記録する１６３４。

【０１７９】さらに、使用するマスターキーの世代番号、すなわち、自身が格納するマスターキーの世代番号［記録時世代番号（Generation#n）］１６５０を取得して、これを記録媒体１６２０に記録時世代番号１６５１として格納する。

【０１８０】ディスク上には、どこのデータがどんなタイトルを構成するかという情報が格納されたデータ管理ファイルがあり、このファイルにタイトルキー１６０５、再生機器制限フラグ１６３５、デバイスＩＤ１６３４、マスターキーの世代番号［記録時世代番号（Generation#n）］１６５１を格納することができる。

【０１８１】なお、記録媒体１６２０には、予め、プレ（pre-recording）世代番号が格納されており、プレ世代番号と同一またはプレ世代番号より新しい世代のマスターキーを用いて暗号化されて格納されたコンテンツのみの再生を可能とする構成となっている。この構成については、後段の再生処理の欄で説明する。

【０１８２】次にディスク固有キー（Disc Unique Key）とタイトルキー（Title Key）と、デバイスＩＤ、あるいは、ディスク固有キー（Disc Unique Key）とタイトルキー（Title Key）と、デバイス固有キー、いずれかの組合せから、タイトル固有キー（Title Unique Key）を生成する。

【０１８３】すなわち、再生機器制限をしない場合には、ディスク固有キー（Disc UniqueKey）とタイトルキー（Title Key）と、デバイスＩＤとからタイトル固有キー（Title Unique Key）を生成し、再生機器制限をする場合には、ディスク固有キー（Disc Unique Key）とタイトルキー（Title Key）と、デバイス固有キーとからタイトル固有キー（Title Unique Key）を生成する。

【０１８４】このタイトル固有キー（Title Unique Key）生成の具体的な方法は、図２１に示すように、ブロック暗号関数を用いたハッシュ関数にタイトルキー（Title Key）とディスク固有キー（Disc Unique Key）と、デバイスＩＤ（再生機器制限をしない場合）もしくはデバイス固有キー（再生機器制限をする場合）を入力して得られた結果を用いる例１の方法や、FIPS 180-1で定められているハッシュ関数ＳＨＡ－１に、マスターキーとディスクＩＤ（Disc ID）とデバイスＩＤ（再生機器制限をしない場合）もしくはデバイス固有キー（再生機器制限をする場合）とのビット連結により生成されるデータを入力し、その１６０ビットの出力から必要なデータ長のみをタイトル固有キー（Title Unique Key）として使用する例２の方法が適用できる。

【０１８５】なお、上記の説明では、マスターキー（Master Key）とディスクＩＤ（Disc ID）からディスク固有キー（Disc Unique Key）を生成し、これとタイトルキー（Title Key）とデバイスＩＤ、もしくはタイトルキー（Title Key）とデバイス固有キーからタイトル固有キー（Title Unique Key）をそれぞれ生成するようにしているが、ディスク固有キー（Disc Unique Key）を不要としてマスターキー（Master Key）とディスクＩＤ（Disc ID）とタイトルキー（Title Key）と、デバイスＩＤもしくはデバイス固有キーから直接タイトル固有キー（Title Unique Key）を生成してもよく、また、タイトルキー（Title Key）を用いずに、マスターキー（Master Key）とディスクＩＤ（Disc ID）と、デバイスＩＤ（再生機器制限をしない場合）もしくはデバイス固有キー（再生機器制限をする場合）からタイトル固有キー（Title Unique Key）相当の鍵を生成してもよい。

【０１８６】ところで、たとえば上記の５ＣＤＴＣＰに規定される伝送フォーマットのひとつを使用した場合、データはＭＰＥＧ２のＴＳパケットで伝送される場合がある。たとえば、衛星放送を受信したセットトップボックス（ＳＴＢ：Set Top Box）がこの放送を記録機に５ＣＤＴＣＰを用いて伝送する際に、ＳＴＢは衛星放送通信路で伝送されたＭＰＥＧ２　ＴＳパケットをＩＥＥＥ１３９４上も伝送することが、データ変換の必要がなく望ましい。

【０１８７】記録再生装置１６００は記録すべきコンテンツデータをこのＴＳパケットの形で受信し、前述したＴＳ処理手段３００において、各ＴＳパケットを受信した時刻情報であるＡＴＳを付加する。なお、先に説明し

たように、ブロックデータに付加されるブロック・シードは、ＡＴＳとコピー制御情報、さらに他の情報を組み合わせた値から構成してもよい。

【０１８８】ＡＴＳを付加したＴＳパケットをＸ個（例えばＸ＝３２）並べて、１ブロックのブロックデータが形成（図５の上の図参照）され、図１６、１７の下段に示すように、被暗号化データとして入力されるブロックデータの先頭の第1～４バイトが分離され（セレクタ１６０８）て出力される３２ビットのＡＴＳを含むブロックシード（Block Seed）と、先に生成したタイトル固有キー（Title Unique Key）とから、そのブロックのデータを暗号化する鍵であるブロック・キー（Block Key）が生成１６０７される。

【０１８９】ブロック・キー（Block Key）の生成方法の例を図２２に示す。図２２では、いずれも３２ビットのブロック・シード（Block Seed）と、６４ビットのタイトル固有キー（Title Unique Key）とから、６４ビットのブロックキー（Block Key）を生成する例を２つ示している。

【０１９０】上段に示す例１は、鍵長６４ビット、入出力がそれぞれ６４ビットの暗号関数を使用している。タイトル固有キー（Title Unique Key）をこの暗号関数の鍵とし、ブロックシード（Block Seed）と３２ビットの定数（コンスタント）を連結した値を入力して暗号化した結果をブロックキー（Block Key）としている。

【０１９１】例２は、FIPS 180-1のハッシュ関数SHA-1を用いた例である。タイトル固有キー（Title Unique Key）とブロックシード（Block Seed）を連結した値をＳＨＡ－１に入力し、その１６０ビットの出力を、たとえば下位６４ビットのみ使用するなど、６４ビットに縮約したものをブロックキー（Block Key）としている。

【０１９２】なお、上記ではディスク固有キー（Disc Unique key）、タイトル固有キー（Title Unique Key）、ブロックキー（Block Key）をそれぞれ生成する例を説明したが、たとえば、ディスク固有キー（Disc Unique Key）とタイトル固有キー（Title Unique Key）の生成を実行することなく、ブロックごとにマスターキー（Master Key）とディスクＩＤ（Disc ID）とタイトルキー（Title Key）とブロックシード（Block Seed）と、デバイスＩＤ（再生機器制限をしない場合）もしくはデバイス固有キー（再生機器制限をする場合）を用いてブロックキー（BlockKey）を生成してもよい。

【０１９３】ブロックキーが生成されると、生成されたブロックキー（Block Key）を用いてブロックデータを暗号化する。図１６、１７の下段に示すように、ブロックシード（Block Seed）を含むブロックデータの先頭の第1～mバイト（たとえばm＝８バイト）は分離（セレクタ１６０８）されて暗号化対象とせず、ｍ＋１バイト目から最終データまでを暗号化１６０９する。なお、暗号化されないmバイト中にはブロック・シードとしての第1～４バイトも含まれる。セレクタ１６０８により分離された第ｍ＋１バイト以降のブロックデータは、暗号処理手段１５０に予め設定された暗号化アルゴリズムに従って暗号化１６０９される。暗号化アルゴリズムとしては、たとえばFIPS 46-2で規定されるＤＥＳ（Data EncryptionStandard）を用いることができる。

【０１９４】ここで、使用する暗号アルゴリズムのブロック長（入出力データサイズ）がＤＥＳのように８バイトであるときは、Ｘを例えば３２とし、mを例えば８の倍数とすることで、端数なくｍ＋１バイト目以降のブロックデータ全体が暗号化できる。

【０１９５】すなわち、１ブロックに格納するＴＳパケットの個数をＸ個とし、暗号アルゴリズムの入出力データサイズをＬバイトとし、ｎを任意の自然数とした場合、１９２＊Ｘ＝ｍ＋ｎ＊Ｌが成り立つようにＸ，ｍ、Ｌを定めることにより、端数処理が不要となる。

【０１９６】暗号化した第ｍ＋１バイト以降のブロックデータは暗号処理のされていない第1～mバイトデータとともにセレクタ１６１０により結合されて暗号化コンテンツ１６１２として記録媒体１６２０に格納される。

【０１９７】以上の処理により、コンテンツはブロック単位で、世代管理されたマスターキー、ＡＴＳを含むブロック・シード等に基づいて生成されるブロック鍵で暗号化が施されて記録媒体に格納される。

【０１９８】上述のように、本構成では、世代管理されたマスターキーによりコンテンツデータが暗号化され記録媒体に格納されているので、その記録媒体を他の記録再生器における再生処理は、少なくとも同一世代、あるいはデータを記録した際に使用されたマスターキーの世代より新しい世代を有する記録再生器であることが復号、すなわち再生可能となる条件となる。

【０１９９】さらに、ブロックキーは上述のように再生機器制限をしない場合は、デバイスＩＤに基づいて生成され、再生機器制限をする場合は、デバイス固有キーに基づいて生成される。これらの暗号化データは、再生機器制限をした場合は、そのデータを記録した機器でのみ再生可能となる。

【０２００】すなわち、再生機器制限なしの場合は、ブロックデータの暗号化鍵であるブロックキーが、デバイスＩＤを含むデータに基づいて生成されるとともに、デバイスＩＤが記録媒体に格納される。従って、記録媒体上のコンテンツを再生しようとする機器は、記録媒体からデバイスＩＤを取得可能であり、同様のブロックキーを生成することが可能となるのでブロックデータの復号が可能となる。しかし、再生機器制限ありの場合は、ブロックデータの暗号化鍵であるブロックキーが、デバイス固有キーを含むデータに基づいて生成される。このデバイス固有キーはデバイス毎に異なる秘密鍵であり、他の機器は、そのキーを取得することはできない。また、ブロックデータを暗号化して記録媒体に格納する場合、

デバイス固有キーの記録媒体に対する書き込み処理は実行されない。従って、他の再生機器では、暗号化されたブロックデータを格納した記録媒体を装着しても、同一のデバイス固有キーを取得することができないので、ブロックデータを復号するための復号キーを生成することができず、復号不可能となり再生できない。なお、再生処理の詳細については後述する。

【０２０１】次に図１８に示すフローチャートに従って、データ記録処理にともなって実行されるＴＳ処理手段３００におけるＡＴＳ付加処理および暗号処理手段１５０における暗号処理の処理の流れを説明する。図１８のＳ１８０１において、記録再生装置は自身のメモリ１８０に格納しているマスターキー、デバイス識別子としてのデバイスＩＤ、デバイス固有キーを読み出す。

【０２０２】Ｓ１８０２において、記録媒体に識別情報としてのディスクＩＤ（Disc ID）が既に記録されているかどうかを検査する。記録されていればＳ１８０３でこのディスクＩＤを読出し、記録されていなければＳ１８０４で、ランダムに、もしくはあらかじめ定められた方法でディスクＩＤを生成し、ディスクに記録する。次に、Ｓ１８０５では、マスタキーとディスクＩＤを用いて、ディスク固有キーを生成する。ディスク固有キーは先に説明したように、例えば、FIPS 180-1で定められているハッシュ関数ＳＨＡ－１を用いる方法やブロック暗号に基づくハッシュ関数を使用する方法などを適用することで求める。

【０２０３】次にＳ１８０６に進み、その一回の記録ごとの固有の鍵としてのタイトルキー（Title Key）、再生機器制限フラグ（Player Restriction Flag）、さらに、機器識別情報としてのデバイスＩＤ、マスターキーの世代番号を取り出してディスクに記録する。次にＳ１８０７で、上記のディスク固有キーとタイトルキーと、デバイスＩＤ（再生機器制限をしない場合）もしくはデバイス固有キー（再生機器制限をする場合）から、タイトル固有キーを生成する。

【０２０４】タイトル固有キーの生成の詳細フローを図２０に示す。暗号処理手段１５０は、ステップＳ２００１において、再生機器制限をするかしないかの判定を実行する。この判定は、記録再生器を使用するユーザによって入力された指示データ、あるいはコンテンツに付加された利用制限情報に基づいて判定する。

【０２０５】Ｓ２００１の判定がＮｏ、すなわち、再生機器制限をしない場合は、ステップＳ２００２に進み、ディスク固有キー（Disc Unique Key）とタイトルキー（Title Key）と、デバイスＩＤとから、タイトル固有キー（Title Unique Key）を生成する。

【０２０６】Ｓ２００１の判定がＹｅｓ、すなわち、再生機器制限をする場合は、ステップＳ２００３に進みディスク固有キー（Disc Unique Key）とタイトルキー（TitleKey）と、デバイス固有キーとから、タイトル固有キー（Title Unique Key）を生成する。キー生成には、ＳＨＡ－１を用いる方法やブロック暗号に基づくハッシュ関数を使用する。

【０２０７】Ｓ１８０８では、記録再生装置は記録すべきコンテンツデータの被暗号化データをＴＳパケットの形で受信する。Ｓ１８０９で、ＴＳ処理手段３００は、各ＴＳパケットを受信した時刻情報であるＡＴＳを付加する。あるいはコピー制御情報ＣＣＩとＡＴＳ、さらに他の情報を組み合わせた値を付加する。次に、Ｓ１８１０で、ＡＴＳを付加したＴＳパケットを順次受信し、１ブロックを形成する例えばＸ＝３２に達したか、あるいはパケットの終了を示す識別データを受信したかを判定する。いずれかの条件が満足された場合はステップＳ１８１１に進み、Ｘ個、あるいはパケット終了までのパケットを並べて、１ブロックのブロックデータを形成する。

【０２０８】次に、暗号処理手段１５０は、Ｓ１８１２で、ブロックデータの先頭の３２ビット（ＡＴＳを含むブロック・シード）とＳ１８０７で生成したタイトル固有キーとから、そのブロックのデータを暗号化する鍵であるブロックキーを生成する。

【０２０９】Ｓ１８１３では、ブロックキーを用いてＳ１８１１で形成したブロックデータを暗号化する。なお、先にも説明したように、暗号化の対象となるのは、ブロックデータのｍ＋１バイト目から最終データまでである。暗号化アルゴリズムは、たとえばFIPS 46-2で規定されるＤＥＳ（Data Encryption Standard）が適用される。

【０２１０】Ｓ１８１４で、暗号化したブロックデータを記録媒体に記録する。Ｓ１８１５で、全データを記録したかを判断する。全データを記録していれば、記録処理を終了し、全データを記録していなければＳ１８０８に戻って残りのデータの処理を実行する。

【０２１１】［世代管理のなされたマスターキーによるコンテンツデータ復号および再生処理］次に、上記のようにして記録媒体に記録された暗号化コンテンツを復号して再生する処理について図２３の処理ブロック図と、図２４～図２６のフローチャートを用いて説明する。

【０２１２】図２３の処理ブロック図を参照しながら、図２４に示すフローチャートに従って、復号処理および再生処理について、処理の流れを説明する。図２４のＳ２４０１において、記録再生装置２３００はディスク２３２０からディスクＩＤ２３０２とプレ（pre-recording）記録世代番号を読み出し、また自身のメモリからマスターキー２３０１、デバイス識別子としてのデバイスＩＤ２３３１、デバイス固有キー２３３２を読み出す。先の記録処理の説明から明らかなように、ディスクＩＤはディスクにあらかじめ記録されているか、そうでない場合は記録再生器において生成してディスクに記録したディスク固有の識別子である。

【０２１３】プレ（pre－recording）記録世代番号２３６０は、予め記録媒体であるディスクに格納されたディスク固有の世代情報である。このプレ（pre－recording）世代番号と、データ記録時のマスターキーの世代番号、すなわち記録時世代番号２３５０を比較して再生処理の可否を制御する。マスターキー２３０１は、ライセンスを受けた記録再生装置に格納され世代管理のなされた秘密キーであり、デバイスＩＤは記録再生装置固有の識別子、デバイス固有キーは、その記録再生器に固有の秘密鍵である。

【０２１４】記録再生装置２３００は、次に、Ｓ２４０２で、ディスクから読み出すべきデータのタイトルキー、さらに、このデータを記録した記録再生器のデバイスＩＤと、データに対応して設定された再生機器制限フラグ、データを記録したときに使用したマスターキーの世代番号（Generation #）すなわち記録時世代番号２３５０を読み出す。次に、Ｓ２４０３で読み出すべきデータが再生可能か否かを判定する。判定の詳細フローを図２５に示す。

【０２１５】図２５のステップＳ２５０１において、記録再生装置は、Ｓ２４０１で読み出したプレ世代番号と、Ｓ２４０２で読み出した記録時世代番号の新旧を判定する。記録時世代番号が示す世代が、プレ記録世代情報が表す世代以後でないと判定された場合、即ち、データ記録時世代情報が表す世代が、プレ記録世代情報が表す世代よりも古い世代である場合、再生不可能と判断し、ステップＳ２４０４乃至Ｓ２４０９をスキップして、再生処理を行わずに処理を終了する。従って、記録媒体に記録されたコンテンツが、プレ記録世代情報が表す世代よりも古い世代のマスターキーに基づいて暗号化されたものである場合には、その再生は許可されず、再生は行われない。

【０２１６】即ち、この処理は、不正が発覚して、最新の世代のマスターキーが与えられなくなった不正な記録装置で、古い世代のマスターキーに基づいて、データが暗号化され、記録媒体に記録された場合に該当するものと判断し、そのような不正な装置によってデータが記録された記録媒体の再生は行わないとした処理である。これにより、不正な記録装置の使用を排除することができる。

【０２１７】一方、ステップＳ２５０１において、記録時世代番号が表す世代が、プレ記録世代番号が表す世代以後であると判定された場合、即ち、記録時世代情報が表す世代が、プレ記録世代番号が表す世代ｎと同一か、または新しい世代であり、従って、記録媒体に記録されたコンテンツが、プレ記録世代情報が表す世代以後の世代のマスターキーに基づいて暗号化されたものである場合には、ステップＳ２５０２に進み、記録再生装置は、自身のメモリが記憶している暗号化マスターキーＣの世代情報を取得し、その暗号化マスターキーの世代と、暗号時世代情報が表す世代を比較して、その世代の前後を判定する。

【０２１８】ステップＳ２５０２において、メモリに記憶されたマスターキーＣの世代が、記録時世代情報が表す世代以後でないと判定された場合、即ち、メモリに記憶されたマスターキーＣの世代が、記録時世代情報が表す世代よりも古い世代である場合、再生不可能と判断し、ステップＳ２４０４乃至Ｓ２４０９をスキップして、再生処理を行わずに処理を終了する。

【０２１９】一方、ステップＳ２５０２において、メモリに記憶された暗号化マスターキーＣの世代が、記録時世代情報が表す世代以後であると判定された場合、即ち、メモリに記憶されたマスターキーＣの世代が、記録時世代情報が表す世代と同一か、またはそれよりも新しい場合、ステップＳ２５０３に進み、読出しをしたいデータが再生機器制限されて記録されているかどうかを検査する。

【０２２０】ステップＳ２５０３では、読み出した再生機器制限フラグの示す再生機器制限情報が、「再生機器制限あり」の設定であるか否かを判定する。ありの場合は、ステップＳ２５０４において、「記録媒体から読み出したデバイスＩＤと自己のデバイスＩＤが一致するか否か」を判定する。一致する場合は、再生可能と判定する。ステップＳ２５０３において、「再生機器制限あり」の設定でないと判定された場合も、再生可能と判定する。読み出した再生機器制限フラグが示す再生機器制限情報が、「再生機器制限あり」かつ、「記録媒体から読み出したデバイスＩＤと自己のデバイスＩＤが一致しない」場合は、再生不可能と判定する。

【０２２１】再生可能と判定された場合は、ステップＳ２４０４に進む。Ｓ２４０４では、ディスクＩＤ（Disc ID）とマスターキー（Master Key）を用いてディスク固有キー（Disc Unique Key）を生成２３０３する。このキー生成方法は、例えば、FIPS 180-1で定められているハッシュ関数SHA-1に、マスターキーとディスクＩＤ（Disc ID）とのビット連結により生成されるデータを入力し、その１６０ビットの出力から必要なデータ長のみをディスク固有キー（Disc Unique Key）として使用する方法や、ブロック暗号関数を用いたハッシュ関数にマスターキー（Master Key）とディスクＩＤ（Disc ID）を入力して得られた結果を用いるなどの方法が挙げられる。ここで使用するマスターキーは、Ｓ２４０２で記録媒体から読み出した、そのデータの記録時世代番号が表す世代（時点）のマスターキーである。もし記録再生装置がこれよりも新しい世代のマスターキーを保持している場合には、前述した方法を用いて記録時世代番号が表す世代のマスターキーを作成し、それを用いてディスク固有キー（Disc Unique Key）を生成してもよい。

【０２２２】次に、Ｓ２４０５で、タイトル固有キーの生成を行なう。タイトル固有キーの生成の詳細フローを

図２６に示す。暗号処理手段１５０は、ステップＳ２６０１において、再生機器制限をするの設定であるか、しないの設定であるかの判定を実行する。この判定は、ディスクから読み出した再生機器制限フラグに基づいて実行される。

【０２２３】データを記録した記録再生器のデバイスＩＤ２３３４と、データに対応して設定された再生機器制限フラグ２３３５を読み出し、読み出した再生機器制限フラグ２３３５が示す再生機器制限情報が、「再生機器制限あり」かつ、「記録媒体から読み出したデバイスＩＤ２３３４と自己のデバイスＩＤ２３３１が一致する」か、あるいは、読み出した再生機器制限フラグ２３３３が示す再生機器制限情報が、「再生機器制限なし」である場合は、再生可能となり、読み出した再生機器制限フラグ２３３３が示す再生機器制限情報が、「再生機器制限あり」かつ、「記録媒体から読み出したデバイスＩＤ２３３４と自己のデバイスＩＤ２３３１が一致しない」場合は、再生不可能となる。

【０２２４】再生不可能とされる場合は、データは、そのデータを記録した記録再生器固有のデバイス固有キーに基づいて生成されたブロックキーによって暗号化されており、そのデータを記録した記録再生器以外の記録再生器は同一のデバイス固有キーを保有しないので、データを復号するためのブロックキーを生成することができない場合である。

【０２２５】再生可能である場合は、ディスク固有キー（Disc Unique Key）とタイトルキー（Title Key）と、デバイスＩＤ、あるいは、ディスク固有キー（Disc UniqueKey）とタイトルキー（Title Key）と、デバイス固有キー、いずれかの組合せから、タイトル固有キー（Title Unique Key）を生成する。

【０２２６】すなわち、再生機器制限をしない設定である場合には、ディスク固有キー（Disc Unique Key）とタイトルキー（Title Key）と、デバイスＩＤとからタイトル固有キー（Title Unique Key）を生成し、再生機器制限をする設定である場合には、ディスク固有キー（Disc Unique Key）とタイトルキー（Title Key）と、自己のデバイス固有キーとからタイトル固有キー（Title Unique Key）を生成する。このキー生成方法としては、ハッシュ関数SHA-1、ブロック暗号関数を用いたハッシュ関数の適用が可能である。

【０２２７】図２６のフローに従って説明する。Ｓ２６０１の判定がＮｏ、すなわち、再生機器制限をしない設定である場合は、ステップＳ２６０２に進み、ディスク固有キー（Disc Unique Key）とタイトルキー（Title Key）と、デバイスＩＤとから、タイトル固有キー（Title Unique Key）を生成する。

【０２２８】Ｓ２６０１の判定がＹｅｓ、すなわち、再生機器制限をする場合は、ステップＳ２６０３に進みディスク固有キー（Disc Unique Key）とタイトルキー（TitleKey）と、自己の記録再生器の有するデバイス固有キーとから、タイトル固有キー（Title Unique Key）を生成する。キー生成には、ＳＨＡ－１を用いる方法やブロック暗号に基づくハッシュ関数を使用する。

【０２２９】なお、上記の説明では、マスターキー（Master Key）とディスクＩＤ（Disc ID）からディスク固有キー（Disc Unique Key）を生成し、これとタイトルキー（Title Key）とデバイスＩＤ、もしくはタイトルキー（Title Key）とデバイス固有キーからタイトル固有キー（Title Unique Key）をそれぞれ生成するようにしているが、ディスク固有キー（Disc Unique Key）を不要としてマスターキー（Master Key）とディスクＩＤ（Disc ID）とタイトルキー（Title Key）と、デバイスＩＤもしくはデバイス固有キーから直接タイトル固有キー（Title Unique Key）を生成してもよく、また、タイトルキー（Title Key）を用いずに、マスターキー（Master Key）とディスクＩＤ（Disc ID）と、デバイスＩＤ（再生機器制限をしない場合）もしくはデバイス固有キー（再生機器制限をする場合）からタイトル固有キー（Title Unique Key）相当の鍵を生成してもよい。

【０２３０】次にＳ２４０６でディスクから暗号化されて格納されている暗号化コンテンツ２３１２から順次ブロックデータ（Block Data）を読み出し、Ｓ２４０７で、ブロックデータの先頭の４バイトのブロック・シード（Block Seed）をセレクタ２３１０において分離して、ブロックシード（Block Seed）と、Ｓ２４０５で生成したタイトル固有キーを用いてブロックキーを生成する。

【０２３１】ブロック・キー（Block Key）の生成方法は、先に説明した図２２の構成を適用することができる。すなわち、３２ビットのブロック・シード（Block Seed）と、６４ビットのタイトル固有キー（Title Unique Key）とから、６４ビットのブロックキー（Block Key）を生成する構成が適用できる。

【０２３２】なお、上記ではディスク固有キー（Disc Unique key）、タイトル固有キー（Title Unique Key）、ブロックキー（Block Key）をそれぞれ生成する例を説明したが、たとえば、ディスク固有キー（Disc Unique Key）とタイトル固有キー（Title Unique Key）の生成を実行することなく、ブロックごとにマスターキー（Master Key）とディスクＩＤ（Disc ID）とタイトルキー（Title Key）と、ブロックシード（Block Seed）と、デバイスＩＤ（再生機器制限をしない場合）もしくはデバイス固有キー（再生機器制限をする場合）を用いてブロックキー（Block Key）を生成してもよい。

【０２３３】ブロックキーが生成されると、次にＳ２４０８で、ブロックキー（Block Key）を用いて暗号化されているブロックデータを復号２３０９し、セレクタ２３０８を介して復号データとして出力する。なお、復号データには、トランスポートストリームを構成する各ト

ランスポートパケットにＡＴＳが付加されており、先に説明したＴＳ処理手段３００において、ＡＴＳに基づくストリーム処理が実行される。その後、データは、使用、たとえば、画像を表示したり、音楽を鳴らしたりすることが可能となる。

【０２３４】このように、ブロック単位で暗号化され記録媒体に格納された暗号化コンテンツはブロック単位でＡＴＳを含むブロック・シードに基づいて生成されるブロック鍵で復号処理が施されて再生が可能となる。ブロックキーを用いて暗号化されているブロックデータを復号し、Ｓ２４０９で、全データを読み出したかを判断し、全データを読み出していれば終了し、そうでなければＳ２４０６に戻り残りのデータを読み出す。

【０２３５】［記録媒体にのみ有効なメディアキーを使用した処理構成］ところで、上記の実施例においては、キー更新ブロックＫＲＢ：Key RenewalBlockを用いて各記録再生装置に対してマスターキーを伝送し、これを用いて記録再生装置がデータの記録、再生を行うとしていた。

【０２３６】マスターキーは、その時点におけるデータの記録全体に有効な鍵であり、ある時点のマスターキーを得ることができた記録再生装置は、その時点およびそれ以前にこのシステムで記録されたデータを復号することが可能になる。ただし、システム全体で有効であるというその性質上、マスターキーが攻撃者に露呈した場合の影響がシステム全体に及ぶという不具合もある。

【０２３７】これに対し、記録媒体のＫＲＢ（Key Renewal Block）を用いて伝送する鍵として、全システムに有効なマスターキーではなく、その記録媒体にのみ有効なメディアキーとすることも可能である。以下に、第２の実施例としてマスターキーの代わりにメディアキーを用いる方式を説明する。ただし、第１の実施例との変更部分のみを説明する。

【０２３８】図２７には、図１３と同様の例として、デバイス０が記録媒体に格納されている t 時点のＫＲＢと自分があらかじめ格納しているリーフキーＫ０００００とノードキーＫ０００，Ｋ００を用いて更新ノードキーＫ（ｔ）００を生成し、それを用いて更新メディアキー：Ｋ（ｔ）mediaを得る様子を示している。ここで得たＫ（ｔ）mediaは、その記録媒体のデータの記録、再生時に使用される。

【０２３９】なお、図２７におけるプレ記録世代番号（Generation #n)は、メディアキーにおいてはマスターキーのように世代の新旧という概念はないので必須ではなくオプションとして設定される。

【０２４０】各記録再生装置は、たとえば、データの記録もしくは再生のために記録媒体が記録再生装置に挿入された際に、図２８に示すフローチャートによってその記録媒体用のメディアキー：Ｋ（ｔ）mediaを計算し、後にその記録媒体へのアクセスに使用する。

【０２４１】図２８のステップＳ２８０１のＫＲＢの読みこみとＳ２８０２のＫＲＢの処理は、それぞれ図１４のステップＳ１４０３およびＳ１４０４と同様の処理である。

【０２４２】ステップＳ２８０３において記録再生装置はメディアキーＫ（ｔ）mediaをノードキー Ｋ（ｔ）００で暗号化した暗号文Ｅｎｃ（Ｋ（ｔ）００，Ｋ（ｔ）media)を記録媒体から読みこみ、ステップＳ２８０４でこれを復号してメディアキーを得る。もしこの記録再生装置が図１１に示すツリー構成のグループから排除、すなわちリボークされていれば、メディアキーを入手できず、その記録媒体への記録および再生が行えない。

【０２４３】次に、記録媒体へのデータの記録の処理を説明するが、メディアキーにおいてはマスターキーのように世代の新旧という概念はないので、第１の実施例において図１５に示した、プレ記録世代情報と記録再生装置自身が格納するマスターキーの世代の比較による記録可能かどうかのチェックは行わず、上記処理においてメディアキーを得られていれば記録を行えると判断する。すなわち、図２９に示す処理フローのようになる。図２９の処理フローは、メディアキーの取得をＳ２９０１で判定し、取得された場合にのみ、ステップＳ２９０２においてコンテンサの記録処理を実行するものである。

【０２４４】［記録媒体にのみ有効なメディアキーを使用したデータの記録処理］コンテンツデータの記録処理の様子を、図３０、３１のブロック図および図３２のフローチャートを用いて説明する。

【０２４５】本実施例では、第１の実施例と同様、記録媒体として光ディスクを例とする。この実施例では、記録媒体上のデータの bit-by-bit コピーを防ぐために、記録媒体固有の識別情報としてのディスクＩＤ(Disc ID)を、データを暗号化する鍵に作用させるようにしている点も同様である。

【０２４６】図３０および図３１は、それぞれ第１の実施例における図１６および図１７に対応する図であり、マスターキー（Master Key）の代わりにメディアキー（Media Key）が使われている点が異なっており、また、マスターキーの世代を示す記録時世代番号（Generation #）を用いていない点が異なっている。図３０および図３１の差異は、図１６、図１７の差異と同様ディスクＩＤの書き込みを実行するかしないかの差異である。

【０２４７】図３２はメディアキーを用いる本実施例におけるデータ記録処理を示すものであり、実施例１の図１８のフローチャートに対応する。以下、図３２の処理フローについて実施例１と異なる点を中心として説明する。

【０２４８】図３２のＳ３２０１において、記録再生装置３０００は自身のメモリに格納している機器識別情報（Device ID）、機器固有鍵（Device Unique Key）と、図２８のＳ２８０４で計算し、一時的に保存しているメ

ディアキーＫ（ｔ）mediaを読み出す。

【０２４９】Ｓ３２０２において、記録再生装置は記録媒体（光ディスク）３０２０に識別情報としてのディスクＩＤ（Disc ID）が既に記録されているかどうかを検査する。記録されていれば、Ｓ３２０３でこのディスクＩＤ（Disc ID）を読出し（図３０に相当）、記録されていなければ、Ｓ３２０４で、ランダムに、もしくはあらかじめ定められた方法でディスクＩＤ（Disc ID）を生成し、ディスクに記録する（図３１に相当）。ディスクＩＤ（Disc ID）はそのディスクにひとつあればよいので、リードインエリアなどに格納することも可能である。いずれの場合でも、次にＳ３２０５に進む。

【０２５０】Ｓ３２０５では、Ｓ３２０１で読み出したメディアキーとディスクＩＤ（DiscID）を用いて、ディスク固有キー（Disc Unique Key）を生成する。ディスク固有キー（Disc Unique Key）の具体的な生成方法としては、第１の実施例で使用した方法と同じ方法で、マスターキーの代わりにメディアキーを使用すればよい。

【０２５１】次にＳ３２０６に進み、その一回の記録ごとに固有の鍵：タイトルキー（Title Key）をランダムに、あるいはあからじめ定められた方法で生成し、ディスクに記録する。同時に、このタイトル（データ）が、記録した機器でのみ再生できるもの（再生機器制限する）か、他の機器でも再生できる（再生機器制限しない）かを表す情報としての再生機器制限フラグ（Player Restriction Flag）と、記録機器が持つ機器識別情報（Device ID）をディスクに記録する。

【０２５２】ディスク上には、どこのデータがどんなタイトルを構成するかという情報が格納されたデータ管理ファイルがあり、このファイルにタイトルキー、再生機器制限フラグ（Player Restriction Flag）、機器識別情報（Device ID）を格納することができる。

【０２５３】ステップＳ３２０７乃至Ｓ３２１５は図１８のＳ１８０７乃至Ｓ１８１５と同様であるため説明を省略する。

【０２５４】なお、上記の説明では、メディアキー（Media Key）とディスクＩＤ（Disc ID）からディスク固有キー（Disc Unique Key）を生成し、これとタイトルキー（Title Key）とデバイスＩＤ、もしくはタイトルキー（Title Key）とデバイス固有キーからタイトル固有キー（Title Unique Key）をそれぞれ生成するようにしているが、ディスク固有キー（Disc Unique Key）を不要としてメディアキー（Media Key）とディスクＩＤ（Disc ID）とタイトルキー（Title Key）と、デバイスＩＤもしくはデバイス固有キーから直接タイトル固有キー（Title Unique Key）を生成してもよく、また、タイトルキー（Title Key）を用いずに、メディアキー（Media Key）とディスクＩＤ（Disc ID）と、デバイスＩＤ（再生機器制限をしない場合）もしくはデバイス固有キー（再生機器制限をする場合）からタイトル固有キー（Title Unique Key）相当の鍵を生成してもよい。

【０２５５】以上のようにして、メディアキーを用いて記録媒体にデータを記録することができる。

【０２５６】［記録媒体にのみ有効なメディアキーを使用したデータの再生処理］次に、上記のようにして記録されたデータを再生する処理の様子を図３３のブロック図と図３４のフローチャートを用いて説明する。

【０２５７】図３３は、第１の実施例における図２３に対応する図であり、マスターキー（Master Key）の変わりにメディアキー（Media Key）が使われ、そのため記録時世代番号（Generation #）が省略されている点が異なっている。

【０２５８】図３４のＳ３４０１において、記録再生装置３４００は記録媒体であるディスク３４２０からディスクＩＤ（Disc ID）を、また自身のメモリから自己の機器識別情報としてデバイスＩＤ（Device ID），自己の機器固有鍵であるデバイス固有キー（Device Unique Key）と、図２８のＳ２８０４で計算し一時的に保存しているメディアキーを読み出す。

【０２５９】なお、この記録媒体の挿入時に、図２８の処理を行い、メディアキーを入手できなかった場合には、再生処理を行わずに終了する。

【０２６０】次にＳ３４０２で、ディスクから読み出すべきデータのタイトルキー（TitleKey）とこのデータを記録した機器のデバイスＩＤ（Device ID）とこのデータの再生機器制限フラグ（Player Restriction Flag）を読み出す。

【０２６１】次にＳ３４０３で、このデータが再生可能であるか否かを判断する。Ｓ３４０３の処理の詳細を図３５に示す。

【０２６２】ステップＳ３５０１ではメディアキー（Media Key）を得られたか否かを判定する。メディアキーを得られなかった場合、再生不可能となり、メディアキーを得られた場合はステップＳ３５０２に進む。ステップＳ３５０２およびＳ３５０３の処理は図２５のＳ２５０３およびＳ２５０４とそれぞれ同じであり、再生機器制限フラグ（Player Restriction Flag）が表す再生機器制限の状態が、「再生機器制限されている」であり、かつ、Ｓ３５０３で記録媒体から読み出した記録した機器のデバイスＩＤ（Device ID）と、Ｓ３４０１でメモリから読み出した自己のデバイスＩＤ（Device ID）により、「記録した機器が自分ではない」という２つの条件が重なった場合には「再生不可能」と判断し、ステップＳ３４０４乃至Ｓ３４０９をスキップして、再生処理を行わずに処理を終了し、一方それ以外の場合には「再生可能」と判断してＳ３４０４に進む。

【０２６３】ステップＳ３４０４乃至Ｓ３４０９の処理は、図２４のＳ２４０４乃至Ｓ２４０９と同様であるため、説明を省略する。

【０２６４】なお、上記の説明では、メディアキー（Me

dia Key）とディスクＩＤ（Disc ID）からディスク固有キー（Disc Unique Key）を生成し、これとタイトルキー（Title Key）とデバイスＩＤ、もしくはタイトルキー（Title Key）とデバイス固有キーからタイトル固有キー（Title Unique Key）をそれぞれ生成するようにしているが、ディスク固有キー（Disc Unique Key）を不要としてメディアキー（Media Key）とディスクＩＤ（Disc ID）とタイトルキー（Title Key）と、デバイスＩＤもしくはデバイス固有キーから直接タイトル固有キー（Title Unique Key）を生成してもよく、また、タイトルキー（Title Key）を用いずに、メディアキー（Media Key）とディスクＩＤ（Disc ID）と、デバイスＩＤ（再生機器制限をしない場合）もしくはデバイス固有キー（再生機器制限をする場合）からタイトル固有キー（Title Unique Key）相当の鍵を生成してもよい。

【０２６５】上記のようにして、記録媒体へのデータの記録および記録媒体からの再生が行える。

【０２６６】［記録再生装置による記録媒体へのキー更新ブロック（ＫＲＢ）格納処理］ところで、上述した例では、キー更新ブロック：ＫＲＢ（Key Renewal Block）が記録媒体にあらかじめ格納されている例を示したが、図３６に示すように、記録再生装置３６００が入出力Ｉ／Ｆ１２０，１４０や、モデム３６０１等を介して他の機器から受信したＫＲＢ（Key Renewal Block）を、最初に記録媒体にデータを記録する際や、記録媒体にデータを記録するたびごとに記録媒体に記録するようにすることもできる。

【０２６７】すなわち、たとえば第１の実施例において、図３７に示すように、記録再生装置はあらかじめ、入出力Ｉ／Ｆ１２０，１４０やモデム３６０１等を介してキー更新ブロック：ＫＲＢ（Key Renewal Block）とマスターキーをノードキーで暗号化した暗号文を入手し、自身の記憶手段であるメモリ１８０等に格納しておき、コンテンツデータの記録媒体に対する記録の際に、図３８に示すフローチャートに従って処理をする構成としてもよい。

【０２６８】図３８の処理フローについて説明する。ステップＳ３８０１において、データを記録しようとする記録媒体にはすでにキー更新ブロック：ＫＲＢ（Key Renewal Block）が記録されているか否かを検査する。すでに記録媒体にキー更新ブロック：ＫＲＢ（Key Renewal Block）が記録されていた場合にはステップＳ３８０２をスキップして終了する（データの記録処理に進む）が、記録されていない場合には、ステップＳ３９０２に進み、図３９に示すように、自身の記憶手段、例えばメモリ１８０に格納しているキー更新ブロック：ＫＲＢ（Key Renewal Block）とマスターキーを暗号化した暗号文を記録媒体に記録する処理を実行する。その処理の実行の後に、コンテンツデータの記録処理に進む。

【０２６９】この方法は、マスターキーに特化したものではなく、たとえば第２の実施例のようにメディアキーを用いる記録方法に適用することももちろん可能である。

【０２７０】［記録処理におけるコピー制御］さて、コンテンツの著作権者等の利益を保護するには、ライセンスを受けた装置において、コンテンツのコピーを制御する必要がある。

【０２７１】即ち、コンテンツを記録媒体に記録する場合には、そのコンテンツが、コピーしても良いもの（コピー可能）かどうかを調査し、コピーして良いコンテンツだけを記録するようにする必要がある。また、記録媒体に記録されたコンテンツを再生して出力する場合には、その出力するコンテンツが、後で、違法コピーされないようにする必要がある。

【０２７２】そこで、そのようなコンテンツのコピー制御を行いながら、コンテンツの記録再生を行う場合の図１または図２の記録再生装置の処理について、図４０および図４１のフローチャートを参照して説明する。

【０２７３】まず、外部からのディジタル信号のコンテンツを、記録媒体に記録する場合においては、図４０（Ａ）のフローチャートにしたがった記録処理が行われる。図４０（Ａ）の処理について説明する。図１の記録再生器１００を例として説明する。ディジタル信号のコンテンツ（ディジタルコンテンツ）が、例えば、IEEE1394シリアルバス等を介して、入出力Ｉ／Ｆ１２０に供給されると、ステップＳ４００１において、入出力Ｉ／Ｆ１２０は、そのディジタルコンテンツを受信し、ステップＳ４００２に進む。

【０２７４】ステップＳ４００２では、入出力Ｉ／Ｆ１２０は、受信したディジタルコンテンツが、コピー可能であるかどうかを判定する。即ち、例えば、入出力Ｉ／Ｆ１２０が受信したコンテンツが暗号化されていない場合（例えば、上述のＤＴＣＰを使用せずに、平文のコンテンツが、入出力Ｉ／Ｆ１２０に供給された場合）には、そのコンテンツは、コピー可能であると判定される。

【０２７５】また、記録再生装置１００がＤＴＣＰに準拠している装置であるとし、ＤＴＣＰに従って処理を実行するものとする。ＤＴＣＰでは、コピーを制御するためのコピー制御情報としての２ビットのＥＭＩ(Encryption Mode Indicator)が規定されている。ＥＭＩが００Ｂ（Ｂは、その前の値が２進数であることを表す）である場合は、コンテンツがコピーフリーのもの(Copy-freely)であることを表し、ＥＭＩが０１Ｂである場合には、コンテンツが、それ以上のコピーをすることができないもの(No-more-copies)であることを表す。さらに、ＥＭＩが１０Ｂである場合は、コンテンツが、１度だけコピーして良いもの(Copy-one-generation)であることを表し、ＥＭＩが１１Ｂである場合には、コンテンツが、コピーが禁止されているもの(Copy-never)であるこ

とを表す。

【０２７６】記録再生装置１００の入出力Ｉ／Ｆ１２０に供給される信号にＥＭＩが含まれ、そのＥＭＩが、Copy-freelyやCopy-one-generationであるときには、コンテンツはコピー可能であると判定される。また、ＥＭＩが、No-more-copiesやCopy-neverであるときには、コンテンツはコピー可能でないと判定される。

【０２７７】ステップＳ４００２において、コンテンツがコピー可能でないと判定された場合、ステップＳ４００３～Ｓ４００５をスキップして、記録処理を終了する。従って、この場合には、コンテンツは、記録媒体１０に記録されない。

【０２７８】また、ステップＳ４００２において、コンテンツがコピー可能であると判定された場合、ステップＳ４００３に進み、以下、ステップＳ４００３～Ｓ４００５において、図３（Ａ）のステップＳ３０２、Ｓ３０３、Ｓ３０４における処理と同様の処理が行われる。すなわち、ＴＳ処理手段３００によるトランスポートパケットに対するＡＴＳ付加、暗号処理手段１５０における暗号化処理が実行され、その結果得られる暗号化コンテンツを、記録媒体１９５に記録して、記録処理を終了する。

【０２７９】なお、ＥＭＩは、入出力Ｉ／Ｆ１２０に供給されるディジタル信号に含まれるものであり、ディジタルコンテンツが記録される場合には、そのディジタルコンテンツとともに、ＥＭＩ、あるいは、ＥＭＩと同様にコピー制御状態を表す情報（例えば、ＤＴＣＰにおけるembedded CCIなど）も記録される。

【０２８０】この際、一般的には、Copy-One-Generationを表す情報は、それ以上のコピーを許さないよう、No-more-copiesに変換されて記録される。

【０２８１】本発明の記録再生装置では、このＥＭＩやembedded CCIなどのコピー制御情報を、ＴＳパケットに付加する形で記録する。即ち、図１０の例２や例３のように、ＡＴＳを２４ビットないし３０ビット分と、コピー制御情報を加えた３２ビットを図５に示すように各ＴＳパケットに付加する。

【０２８２】外部からのアナログ信号のコンテンツを、記録媒体に記録する場合においては、図４０（Ｂ）のフローチャートにしたがった記録処理が行われる。図４０（Ｂ）の処理について説明する。アナログ信号のコンテンツ（アナログコンテンツ）が、入出力Ｉ／Ｆ１４０に供給されると、入出力Ｉ／Ｆ１４０は、ステップＳ４０１１において、そのアナログコンテンツを受信し、ステップＳ４０１２に進み、受信したアナログコンテンツが、コピー可能であるかどうかを判定する。

【０２８３】ここで、ステップＳ４０１２の判定処理は、例えば、入出力Ｉ／Ｆ１４０で受信した信号に、マクロビジョン(Macrovision)信号や、ＣＧＭＳ－Ａ(Copy Generation Management System-Analog)信号が含まれるかどうかに基づいて行われる。即ち、マクロビジョン信号は、ＶＨＳ方式のビデオカセットテープに記録すると、ノイズとなるような信号であり、これが、入出力Ｉ／Ｆ１４０で受信した信号に含まれる場合には、アナログコンテンツは、コピー可能でないと判定される。

【０２８４】また、例えば、ＣＧＭＳ－Ａ信号は、ディジタル信号のコピー制御に用いられるＣＧＭＳ信号を、アナログ信号のコピー制御に適用した信号で、コンテンツがコピーフリーのもの(Copy-freely)、１度だけコピーして良いもの(Copy-one-generation)、またはコピーが禁止されているもの(Copy-never)のうちのいずれであるかを表す。

【０２８５】従って、ＣＧＭＳ－Ａ信号が、入出力Ｉ／Ｆ１４０で受信した信号に含まれ、かつ、そのＣＧＭＳ－Ａ信号が、Copy-freelyやCopy-one-generationを表している場合には、アナログコンテンツは、コピー可能であると判定される。また、ＣＧＭＳ－Ａ信号が、Copy-neverを表している場合には、アナログコンテンツは、コピー可能でないと判定される。

【０２８６】さらに、例えば、マクロビジョン信号も、ＣＧＭＳ－Ａ信号も、入出力Ｉ／Ｆ４で受信した信号に含まれない場合には、アナログコンテンツは、コピー可能であると判定される。

【０２８７】ステップＳ４０１２において、アナログコンテンツがコピー可能でないと判定された場合、ステップＳ４０１３乃至Ｓ４０１７をスキップして、記録処理を終了する。従って、この場合には、コンテンツは、記録媒体１０に記録されない。

【０２８８】また、ステップＳ４０１２において、アナログコンテンツがコピー可能であると判定された場合、ステップＳ４０１３に進み、以下、ステップＳ４０１３乃至Ｓ４０１７において、図３（Ｂ）のステップＳ３２２乃至Ｓ３２６における処理と同様の処理が行われ、これにより、コンテンツがデジタル変換、ＭＰＥＧ符号化、ＴＳ処理、暗号化処理がなされて記録媒体に記録され、記録処理を終了する。

【０２８９】なお、入出力Ｉ／Ｆ１４０で受信したアナログ信号に、ＣＧＭＳ－Ａ信号が含まれている場合に、アナログコンテンツを記録媒体に記録するときには、そのＣＧＭＳ－Ａ信号も、記録媒体に記録される。即ち、図１０で示したＣＣＩもしくはその他の情報の部分に、この信号が記録される。この際、一般的には、Copy-One-Generationを表す情報は、それ以上のコピーを許さないよう、No-more-copiesに変換されて記録される。ただし、システムにおいてたとえば「Copy-one-generationのコピー制御情報は、No-more-copiesに変換せずに記録するが、No-more-copiesとして扱う」などのルールが決められている場合は、この限りではない。

【０２９０】［再生処理におけるコピー制御］次に、記録媒体に記録されたコンテンツを再生して、ディジタル

コンテンツとして外部に出力する場合においては、図４１（Ａ）のフローチャートにしたがった再生処理が行われる。図４１（Ａ）の処理について説明する。まず最初に、ステップＳ４１０１、Ｓ４１０２、Ｓ４１０３において、図４（Ａ）のステップＳ４０１、Ｓ４０２、Ｓ４０３における処理と同様の処理が行われ、これにより、記録媒体から読み出された暗号化コンテンツが暗号処理手段１５０において復号処理がなされ、ＴＳ処理がなされる。各処理が実行されたディジタルコンテンツは、バス１１０を介して、入出力Ｉ／Ｆ１２０に供給される。

【０２９１】入出力Ｉ／Ｆ１２０は、ステップＳ４１０４において、そこに供給されるディジタルコンテンツが、後でコピー可能なものかどうかを判定する。即ち、例えば、入出力Ｉ／Ｆ１２０に供給されるディジタルコンテンツにＥＭＩ、あるいは、ＥＭＩと同様にコピー制御状態を表す情報（コピー制御情報）が含まれない場合には、そのコンテンツは、後でコピー可能なものであると判定される。

【０２９２】また、例えば、入出力Ｉ／Ｆ１２０に供給されるディジタルコンテンツにＥＭＩが含まれる場合、従って、コンテンツの記録時に、ＤＴＣＰの規格にしたがって、ＥＭＩが記録された場合には、そのＥＭＩ（記録されたＦＭＩ(Recorded EMI)）が、Copy-freelyであるときには、ディジタルコンテンツは、後でコピー可能なものであると判定される。また、ＥＭＩが、No-more-copiesであるときには、コンテンツは、後でコピー可能なものでないと判定される。

【０２９３】なお、一般的には、記録されたＥＭＩが、Copy-one-generationやCopy-neverであることはない。Copy-one-generationのＥＭＩは記録時にNo-more-copiesに変換され、また、Copy-neverのＥＭＩを持つディジタルコンテンツは、記録媒体に記録されないからである。ただし、システムにおいてたとえば「Copy-one-generationのコピー制御情報は、No-more-copiesに変換せずに記録するが、No-more-copiesとして扱う」などのルールが決められている場合は、この限りではない。

【０２９４】ステップＳ４１０４において、コンテンツが、後でコピー可能なものであると判定された場合、ステップＳ４１０５に進み、入出力Ｉ／Ｆ１２０は、そのディジタルコンテンツを、外部に出力し、再生処理を終了する。

【０２９５】また、ステップＳ４１０４において、コンテンツが、後でコピー可能なものでないと判定された場合、ステップＳ４１０６に進み、入出力Ｉ／Ｆ１２０は、例えば、ＤＴＣＰの規格等にしたがって、ディジタルコンテンツを、そのディジタルコンテンツが後でコピーされないような形で外部に出力し、再生処理を終了する。

【０２９６】即ち、例えば、上述のように、記録されたＥＭＩが、No-more-copiesである場合（もしくは、システムにおいてたとえば「Copy-one-generationのコピー制御情報は、No-more-copiesに変換せずに記録するが、No-more-copiesとして扱う」というルールが決められていて、その条件下で記録されたＥＭＩがCopy-one-generationである場合）には、コンテンツは、それ以上のコピーは許されない。

【０２９７】このため、入出力Ｉ／Ｆ１２０は、ＤＴＣＰの規格にしたがい、相手の装置との間で認証を相互に行い、相手が正当な装置である場合（ここでは、ＤＴＣＰの規格に準拠した装置である場合）には、ディジタルコンテンツを暗号化して、外部に出力する。

【０２９８】次に、記録媒体に記録されたコンテンツを再生して、アナログコンテンツとして外部に出力する場合においては、図４１（Ｂ）のフローチャートにしたがった再生処理が行われる。図４１（Ｂ）の処理について説明する。ステップＳ４１１１乃至Ｓ４１１５において、図４（Ｂ）のステップＳ４２１乃至Ｓ４２５における処理と同様の処理が行われる。すなわち、暗号化コンテンツの読み出し、復号処理、ＴＳ処理、ＭＰＥＧデコード、Ｄ／Ａ変換が実行される。これにより得られるアナログコンテンツは、入出力Ｉ／Ｆ１４０で受信される。

【０２９９】入出力Ｉ／Ｆ１４０は、ステップＳ４１１６において、そこに供給されるコンテンツが、後でコピー可能なものかどうかを判定する。即ち、例えば、記録されていたコンテンツにＥＭＩなどのコピー制御情報がいっしょに記録されていない場合には、そのコンテンツは、後でコピー可能なものであると判定される。

【０３００】また、コンテンツの記録時に、例えばＤＴＣＰの規格にしたがって、ＥＭＩまたはコピー制御情報が記録された場合には、その情報が、Copy-freelyであるときには、コンテンツは、後でコピー可能なものであると判定される。

【０３０１】また、ＥＭＩまたはコピー制御情報が、No-more-copiesである場合、もしくは、システムにおいてたとえば「Copy-one-generationのコピー制御情報は、No-more-copiesに変換せずに記録するが、No-more-copiesとして扱う」というルールが決められていて、その条件下で記録されたＥＭＩまたはコピー制御情報がCopy-one-generationである場合には、コンテンツは、後でコピー可能なものでないと判定される。

【０３０２】さらに、例えば、入出力Ｉ／Ｆ１４０に供給されるアナログコンテンツにＣＧＭＳ－Ａ信号が含まれる場合、従って、コンテンツの記録時に、そのコンテンツとともにＣＧＭＳ－Ａ信号が記録された場合には、そのＣＧＭＳ－Ａ信号が、Copy-freelyであるときには、アナログコンテンツは、後でコピー可能なものであると判定される。また、ＣＧＭＳ－Ａ信号が、Copy-neverであるときには、アナログコンテンツは、後でコピー可能なものでないと判定される。

【０３０３】ステップＳ４１１６において、コンテンツが、後でコピー可能であると判定された場合、ステップＳ４１１７に進み、入出力Ｉ／Ｆ１４０は、そこに供給されたアナログ信号を、そのまま外部に出力し、再生処理を終了する。

【０３０４】また、ステップＳ４１１６において、コンテンツが、後でコピー可能でないと判定された場合、ステップＳ４１１８に進み、入出力Ｉ／Ｆ１４０は、アナログコンテンツを、そのアナログコンテンツが後でコピーされないような形で外部に出力し、再生処理を終了する。

【０３０５】即ち、例えば、上述のように、記録されたＥＭＩ等のコピー制御情報が、No-more-copiesである場合（もしくは、システムにおいてたとえば「Copy-one-generationのコピー制御情報は、No-more-copiesに変換せずに記録するが、No-more-copiesとして扱う」というルールが決められていて、その条件下で記録されたＥＭＩ等のコピー制御情報がCopy-one-generationである場合）には、コンテンツは、それ以上のコピーは許されない。

【０３０６】このため、入出力Ｉ／Ｆ１４０は、アナログコンテンツを、それに、例えば、マクロビジョン信号や、Copy-neverを表すＧＣＭＳ－Ａ信号を付加して、外部に出力する。また、例えば、記録されたＣＧＭＳ－Ａ信号が、Copy-neverである場合にも、コンテンツは、それ以上のコピーは許されない。このため、入出力Ｉ／Ｆ４は、ＣＧＭＳ－Ａ信号をCopy-neverに変更して、アナログコンテンツとともに、外部に出力する。

【０３０７】以上のように、コンテンツのコピー制御を行いながら、コンテンツの記録再生を行うことにより、コンテンツに許された範囲外のコピー（違法コピー）が行われることを防止することが可能となる。

【０３０８】［データ処理手段の構成］なお、上述した一連の処理は、ハードウェアにより行うことは勿論、ソフトウェアにより行うこともできる。即ち、例えば、暗号処理手段１５０は暗号化／復号ＬＳＩとして構成することも可能であるが、汎用のコンピュータや、１チップのマイクロコンピュータにプログラムを実行させることにより行う構成とすることも可能である。同様にＴＳ処理手段３００も処理をソフトウェアによって実行することが可能である。一連の処理をソフトウェアによって行う場合には、そのソフトウェアを構成するプログラムが、汎用のコンピュータや１チップのマイクロコンピュータ等にインストールされる。図４２は、上述した一連の処理を実行するプログラムがインストールされるコンピュータの一実施の形態の構成例を示している。

【０３０９】プログラムは、コンピュータに内蔵されている記録媒体としてのハードディスク４２０５やＲＯＭ４２０３に予め記録しておくことができる。あるいは、プログラムはフロッピー（登録商標）ディスク、ＣＤ－ＲＯＭ(Compact Disc Read Only Memory)，ＭＯ(Magneto optical)ディスク，ＤＶＤ(Digital Versatile Disc)、磁気ディスク、半導体メモリなどのリムーバブル記録媒体４２１０に、一時的あるいは永続的に格納（記録）しておくことができる。このようなリムーバブル記録媒体４２１０は、いわゆるパッケージソフトウエアとして提供することができる。

【０３１０】なお、プログラムは、上述したようなリムーバブル記録媒体４２１０からコンピュータにインストールする他、ダウンロードサイトから、ディジタル衛星放送用の人工衛星を介して、コンピュータに無線で転送したり、ＬＡＮ(Local AreaNetwork)、インターネットといったネットワークを介して、コンピュータに有線で転送し、コンピュータでは、そのようにして転送されてくるプログラムを、通信部４２０８で受信し、内蔵するハードディスク４２０５にインストールすることができる。

【０３１１】コンピュータは、ＣＰＵ(Central Processing Unit)４２０２を内蔵している。ＣＰＵ４２０２には、バス４２０１を介して、入出力インタフェース４２１１が接続されており、ＣＰＵ４２０２は、入出力インタフェース４２１０を介して、ユーザによって、キーボードやマウス等で構成される入力部４２０７が操作されることにより指令が入力されると、それにしたがって、ＲＯＭ(Read Only Memory)４２０３に格納されているプログラムを実行する。

【０３１２】あるいは、ＣＰＵ４２０２は、ハードディスク４２０５に格納されているプログラム、衛星若しくはネットワークから転送され、通信部４２０８で受信されてハードディスク４２０５にインストールされたプログラム、またはドライブ４２０９に装着されたリムーバブル記録媒体４２１０から読み出されてハードディスク４２０５にインストールされたプログラムを、ＲＡＭ(Random Access Memory)４２０４にロードして実行する。

【０３１３】これにより、ＣＰＵ４２０２は、上述したフローチャートにしたがった処理、あるいは上述したブロック図の構成により行われる処理を行う。そして、ＣＰＵ４２０２は、その処理結果を、必要に応じて、例えば、入出力インタフェース４２１１を介して、ＬＣＤ(Liquid CryStal Display)やスピーカ等で構成される出力部４２０６から出力、あるいは、通信部４２０８から送信、さらには、ハードディスク４２０５に記録させる。

【０３１４】ここで、本明細書において、コンピュータに各種の処理を行わせるためのプログラムを記述する処理ステップは、必ずしもフローチャートとして記載された順序に沿って時系列に処理する必要はなく、並列的あるいは個別に実行される処理（例えば、並列処理あるいはオブジェクトによる処理）も含むものである。

【０３１５】また、プログラムは、１のコンピュータにより処理されるものであっても良いし、複数のコンピュ

ータによって分散処理されるものであっても良い。さらに、プログラムは、遠方のコンピュータに転送されて実行されるものであっても良い。

【０３１６】なお、本実施の形態では、コンテンツの暗号化／復号を行うブロックを、１チップの暗号化／復号ＬＳＩで構成する例を中心として説明したが、コンテンツの暗号化／復号を行うブロックは、例えば、図１および図２に示すＣＰＵ１７０が実行する１つのソフトウェアモジュールとして実現することも可能である。同様に、ＴＳ処理手段３００の処理もＣＰＵ１７０が実行する１つのソフトウェアモジュールとして実現することが可能である。

【０３１７】［記録媒体の製造装置および方法］次に、上述した本発明の情報記録媒体を製造する本発明の情報記録媒体製造装置および方法について説明する。

【０３１８】図４３には、記録媒体を製造すると共に、記録媒体に対してディスクＩＤ（Disk ID），キー更新ブロック：ＫＲＢ（Key Renewal Block）および、暗号化されたマスターキーまたは暗号化されたメディアキーを記録するディスク製造装置の概略構成を示す。

【０３１９】この図４３に示すディスク製造装置は、図示しない組立工程により既に組み立てられている情報記録媒体に対して、ディスクＩＤ（Disk ID），キー更新ブロック：ＫＲＢ（Key Renewal Block）および、暗号化されたマスターキーまたは暗号化されたメディアキーを記録する。さらに、必要に応じてマスターキーのプレ（pre－recording）記録世代情報（Generation#n）も併せて記録する。

【０３２０】ディスク製造装置４３００は、ディスクＩＤ（Disk ID），キー更新ブロック：ＫＲＢ（Key Renewal Block）および、暗号化されたマスターキーまたは暗号化されたメディアキーをあらかじめ格納しているメモリ４３０２もしくはその他の記憶手段と、記録媒体４３５０に対する読み書きを行う記録媒体Ｉ／Ｆ４３０３と、他の装置とのＩ／Ｆとなる入出力Ｉ／Ｆ４３０４と、それらを制御する制御部４３０１、これらを接続するバス４３０５を備えている。

【０３２１】なお、図４３の構成では、メモリ４３０２および記録媒体Ｉ／Ｆ４３０４は、当該製造装置に内蔵されている例を挙げているが、メモリ４３０２および記録媒体Ｉ／Ｆ４３０３は外付けのものであってもよい。

【０３２２】上記のディスクＩＤ（Disk ID），キー更新ブロック：ＫＲＢ（Key Renewal Block）および、暗号化されたマスターキーまたは暗号化されたメディアキー、マスターキーのプレ（pre－recording）記録世代情報（Generation#n）は、たとえば図示しない鍵発行センタにより発行されるものであり、上記内蔵あるいは外付けのメモリにあらかじめ格納されている。

【０３２３】上記メモリ４３０２に格納されているディスクＩＤ（Disk ID），キー更新ブロック：ＫＲＢ（Key Renewal Block）および、暗号化されたマスターキーまたは暗号化されたメディアキーは、制御部４３０１の制御の下、記録媒体Ｉ／Ｆ４３０３を介して記録媒体に記録される。なお、必要に応じてマスターキーのプレ（pre－recording）記録世代情報（Generation#n）についても記録する。

【０３２４】また、ディスクＩＤ（Disk ID），キー更新ブロック：ＫＲＢ（Key Renewal Block）および、暗号化されたマスターキーまたは暗号化されたメディアキー、マスターキーのプレ（pre－recording）記録世代情報（Generation#n）は、上述したようにメモリ４３０２にあらかじめ格納されているものを使用するだけでなく、たとえば入出力Ｉ／Ｆ４３０４を介して鍵発行センタから送られてきたものを入手することも可能である。

【０３２５】図４４には、本発明の記録媒体製造方法として、上記記録媒体を製造すると共に、記録媒体に対してディスクＩＤ（Disk ID），キー更新ブロック：ＫＲＢ（Key Renewal Block）および、暗号化されたマスターキーまたは暗号化されたメディアキー、マスターキーのプレ（pre－recording）記録世代情報（Generation#n）を記録する記録媒体製造方法における製造工程の流れを示す。

【０３２６】図４４において、記録媒体製造方法では、まず、ステップＳ４４０１の製造工程として、図示しない公知の組立工程によりＤＶＤ、ＣＤ等各種記録媒体が組み立てられる。

【０３２７】次に、ステップＳ４４０２の製造工程として、図４３の記録媒体製造装置により、製造された記録媒体に対して、ディスクＩＤ（Disk ID），キー更新ブロック：ＫＲＢ（Key Renewal Block）および、暗号化されたマスターキーまたは暗号化されたメディアキーの記録処理を実行する。また、必要に応じてマスターキーのプレ（pre－recording）記録世代情報（Generation#n）を記録する。

【０３２８】以上のディスク製造処理プロセスにより、記録媒体は、ディスクＩＤ（Disk ID），キー更新ブロック：ＫＲＢ（Key Renewal Block）および、暗号化されたマスターキーまたは暗号化されたメディアキーを記録した状態で製造工場から出荷される。また、必要に応じてマスターキーのプレ（pre－recording）記録世代情報（Generation#n）を記録した後、製造工場から出荷される。

【０３２９】［ＫＲＢのフォーマット］図４５にキー更新ブロック（ＫＲＢ：Key Renewal Block）のフォーマット例を示す。バージョン４５０１は、キー更新ブロック（ＫＲＢ：Key Renewal Block）のバージョンを示す識別子である。デプス４５０２は、キー更新ブロック（ＫＲＢ：Key Renewal Block）の配布先のデバイスに対する階層ツリーの階層数を示す。データポインタ４５０３は、キー更新ブロック（ＫＲＢ：Key RenewalBloc

k）中のデータ部の位置を示すポインタであり、タグポインタ４５０４はタグ部の位置、署名ポインタ４５０５は署名の位置を示すポインタである。データ部４５０６は、例えば更新するノードキーを暗号化したデータを格納する。

【０３３０】タグ部４５０７は、データ部に格納された暗号化されたノードキー、リーフキーの位置関係を示すタグである。このタグの付与ルールを図４６を用いて説明する。図４６では、データとして先に図１２（Ａ）で説明したキー更新ブロック（ＫＲＢ）を送付する例を示している。この時のデータは、図４６の右の表に示すようになる。このときの暗号化キーに含まれるトップノードのアドレスをトップノードアドレスとする。この場合は、ルートキーの更新キーＫ（ｔ）Ｒが含まれているので、トップノードアドレスはＫＲとなる。

【０３３１】暗号化キーの最上段のデータＥｎｃ（Ｋ（ｔ）０，Ｋ（ｔ）Ｒ）は、図４６の左の階層ツリーに示す位置にある。ここで、次のデータは、Ｅｎｃ（Ｋ（ｔ）００，Ｋ（ｔ）０）であり、ツリー上では前のデータの左下の位置にある。データがある場合は、タグが０、ない場合は１が設定される。タグは｛左（Ｌ）タグ，右（Ｒ）タグ｝として設定される。最上段のデータＥｎｃ（Ｋ（ｔ）０，Ｋ（ｔ）Ｒ）の左にはデータがあるので、Ｌタグ＝０、右にはデータがないので、Ｒタグ＝１となる。以下、すべてのデータにタグが設定され、図４６（ｃ）に示すデータ列、およびタグ列が構成される。ツリーのノードの処理の順序として同一段の幅方向を先に処理するｗｉｄｔｈ　ｆｉｒｓｔと、深さ方向を先に処理するｄｅｐｔｈ　ｆｉｒｓｔのいずれかを用いるのが好適である。

【０３３２】図４５に戻って、ＫＲＢフォーマットについてさらに説明する。署名（Signature）は、キー更新ブロック（ＫＲＢ）を発行した例えば鍵管理センタ、コンテンツロバイダ、決済機関等が実行する電子署名である。ＫＲＢを受領したデバイスは署名検証によって正当なキー更新ブロック（ＫＲＢ）発行者が発行したキー更新ブロック（ＫＲＢ）であることを確認する。

【０３３３】以上、特定の実施例を参照しながら、本発明について詳解してきた。しかしながら、本発明の要旨を逸脱しない範囲で当業者が該実施例の修正や代用を成し得ることは自明である。すなわち、例示という形態で本発明を開示してきたのであり、限定的に解釈されるべきではない。本発明の要旨を判断するためには、冒頭に記載した特許請求の範囲の欄を参酌すべきである。

【０３３４】

【発明の効果】以上、説明したように、本発明の情報記録再生装置によれば、ツリー（木）構造の鍵配布構成により、マスターキーやメディアキーの更新データを更新ブロック（ＫＲＢ）とともに送信する構成としたので、鍵更新の必要なデバイスにのみ復号可能な構成とした伝送または配布が可能となり、メッセージ量を小さく抑えることができる。さらに、ツリー構造によって規定される特定のグループにのみ復号可能な鍵をメッセージ量を少なくして配布可能であり、グループに属さない他のデバイスには復号できない構成とすることが可能であり、キー配信または配布の安全性が確保される。

【０３３５】また、ツリー構造の鍵配信方式を用いて各記録再生装置に伝送する鍵の種類を、ツリーを構成する特定のグループによって規定されるシステムで共通に利用できるマスターキーとすることも、各記録媒体ごとに固有のメディアキーとすることも可能であり、それぞれに固有のＫＲＢを生成してネットワーク配信、またはメディアを介して配布することにより、キー更新が容易にかつ安全に実行される。

【０３３６】このため、本発明によれば、映画や音楽などの著作権があるデータの不正な（著作権者の意に反する）複製を防ぐことができる情報記録再生システムを構成することが可能である。

【０３３７】また、世代管理を行なったマスターキーを使用するシステムにおいて、ＫＲＢにより更新された新たな世代のマスターキーを配布する構成とすることにより、ＫＲＢとともに暗号化されて配布される更新マスターキーを更新可能なデバイスを特定した固有のキーブロックを構成可能であるので、従来のデバイス単位での認証処理等を実行することなく、安全に更新の必要なデバイスのみが復号可能な暗号化マスターキーを構成して安全に鍵更新が実行できる。

【０３３８】さらに、本発明の情報記録再生装置および方法によれば、世代管理されたマスターキー、あるいはメディアキーによる暗号化処理のみならず、再生機器制限処理を可能とした暗号処理を実行して記録媒体に格納する構成としている。本構成によって、データを記録媒体に記録する際に、その機器でのみ再生できるようにする（再生機器制限する）場合には機器固有鍵（デバイス固有キー）をデータの暗号鍵に作用させ、そうでない（再生機器制限しない）場合には機器識別情報（デバイスＩＤ）をデータの暗号鍵に作用させて暗号化するようにする。さらに、記録した機器の機器識別情報と、再生機器制限したかしないかのどちらのモードで記録したかを表す情報（再生機器制限フラグ）を記録媒体に記録しておく構成としたので、データの再生時に、再生機器制限されている場合には機器固有鍵を知っている記録した機器のみがデータを復号でき、再生機器制限されていない場合にはいずれの機器でも記録機器の機器識別情報を用いてデータを復号できるようになる。

【０３３９】また、各パケットの着信時刻に応じたランダム性のあるデータとして構成されるＡＴＳを用いてブロック・データを暗号化するブロックキーを生成する構成としたので、ブロック毎に異なる固有キーを生成することが可能となり、ブロックごとに暗号鍵を変更でき、

暗号解析に対する強度を高めることができる。また、ＡＴＳを用いてブロックキーを生成する構成とすることにより、各ブロック毎の暗号化鍵を格納するための記録媒体上の領域が不要となり、メインデータ領域が有効に使用可能となる。さらに、データの記録、再生時にメインデータ部以外のデータをアクセスする必要もなくなり、処理が効率的になる。

【図面の簡単な説明】

【図１】本発明の情報記録再生装置の構成例（その１）を示すブロック図である。

【図２】本発明の情報記録再生装置の構成例（その２）を示すブロック図である。

【図３】本発明の情報記録再生装置のデータ記録処理フローを示す図である。

【図４】本発明の情報記録再生装置のデータ再生処理フローを示す図である。

【図５】本発明の情報記録再生装置において処理されるデータフォーマットを説明する図である。

【図６】本発明の情報記録再生装置におけるトランスポート・ストリーム（ＴＳ）処理手段の構成を示すブロック図である。

【図７】本発明の情報記録再生装置において処理されるトランスポート・ストリームの構成を説明する図である。

【図８】本発明の情報記録再生装置におけるトランスポート・ストリーム（ＴＳ）処理手段の構成を示すブロック図である。

【図９】本発明の情報記録再生装置におけるトランスポート・ストリーム（ＴＳ）処理手段の構成を示すブロック図である。

【図１０】本発明の情報記録再生装置において処理されるブロックデータの付加情報としてのブロック・データの構成例を示す図である。

【図１１】本発明の情報記録再生装置に対するマスターキー、メディアキー等の鍵の暗号化処理について説明するツリー構成図である。

【図１２】本発明の情報記録再生装置に対するマスターキー、メディアキー等の鍵の配布に使用されるキー更新ブロック（ＫＲＢ）の例を示す図である。

【図１３】本発明の情報記録再生装置におけるマスターキーのキー更新ブロック（ＫＲＢ）を使用した配布例と復号処理例を示す図である。

【図１４】本発明の情報記録再生装置におけるマスターキーのキー更新ブロック（ＫＲＢ）を使用した復号処理フローを示す図である。

【図１５】本発明の情報記録再生装置におけるコンテンツ記録処理におけるマスターキーの世代比較処理フローを示す図である。

【図１６】本発明の情報記録再生装置において、再生機器制限可能なシステムにおけるデータ記録処理時の暗号化処理を説明するブロック図（その１）である。

【図１７】本発明の情報記録再生装置において、再生機器制限可能なシステムにおけるデータ記録処理時の暗号化処理を説明するブロック図（その２）である。

【図１８】本発明の情報記録再生装置において、再生機器制限可能なシステムにおけるデータ記録処理を説明するフローチャートである。

【図１９】本発明の情報記録再生装置におけるディスク固有キーの生成例を説明する図である。

【図２０】本発明の情報記録再生装置において、再生機器制限可能なシステムにおけるタイトル固有キーの生成処理フローを示す図である。

【図２１】本発明の情報記録再生装置において、再生機器制限可能なシステムにおけるデータ記録時のタイトル固有キーの生成処理例を示す図である。

【図２２】本発明の情報記録再生装置におけるブロック・キーの生成方法を説明する図である。

【図２３】本発明の情報記録再生装置において、再生機器制限可能なシステムにおけるデータ再生処理時の復号処理を説明するブロック図である。

【図２４】本発明の情報記録再生装置において、再生機器制限可能なシステムにおけるデータ再生処理を説明するフローチャートである。

【図２５】本発明の情報記録再生装置において、再生機器制限可能なシステムにおけるデータ再生処理における再生可能制判定処理の詳細を示すフローチャートである。

【図２６】本発明の情報記録再生装置において、再生機器制限可能なシステムにおけるデータ最盛時のタイトル固有キーの生成処理フローを示す図である。

【図２７】本発明の情報記録再生装置におけるメディアキーのキー更新ブロック（ＫＲＢ）を使用した配布例と復号処理例を示す図である。

【図２８】本発明の情報記録再生装置におけるメディアキーのキー更新ブロック（ＫＲＢ）を使用した復号処理フローを示す図である。

【図２９】本発明の情報記録再生装置におけるメディアキーを使用したコンテンツ記録処理フローを示す図である。

【図３０】本発明の情報記録再生装置において、再生機器制限可能なシステムにおけるメディアキーを使用したデータ記録処理時の暗号化処理を説明するブロック図（その１）である。

【図３１】本発明の情報記録再生装置において、再生機器制限可能なシステムにおけるメディアキーを使用したデータ記録処理時の暗号化処理を説明するブロック図（その２）である。

【図３２】本発明の情報記録再生装置において、再生機器制限可能なシステムにおけるメディアキーを使用したデータ記録処理を説明するフローチャートである。

【図３３】本発明の情報記録再生装置において、再生機器制限可能なシステムにおけるメディアキーを使用したデータ再生処理時の暗号化処理を説明するブロック図である。

【図３４】本発明の情報記録再生装置において、再生機器制限可能なシステムにおけるメディアキーを使用したデータ再生処理を説明するフローチャートである。

【図３５】本発明の情報記録再生装置において、再生機器制限可能なシステムにおけるメディアキーを使用したデータ再生処理における再生可能制判定処理の詳細を示すフローチャートである。

【図３６】本発明の情報記録再生装置において、外部からＫＲＢを通信手段等を介して受信し、記録媒体に格納する構成とした記録再生装置構成を示すブロック図である。

【図３７】本発明の情報記録再生装置において、外部からＫＲＢを通信手段等を介して受信し、記録媒体に格納する処理について示すブロック図である。

【図３８】本発明の情報記録再生装置において、外部からＫＲＢを通信手段等を介して受信し、記録媒体に格納する処理フローを示すブロック図である。

【図３９】本発明の情報記録再生装置において、外部からＫＰＢを通信手段等を介して受信し、記録媒体に格納する処理を説明する図である。

【図４０】本発明の情報記録再生装置におけるデータ記録処理時のコピー制御処理を説明するフローチャートである。

【図４１】本発明の情報記録再生装置におけるデータ再生処理時のコピー制御処理を説明するフローチャートである。

【図４２】本発明の情報記録再生装置において、データ処理をソフトウェアによって実行する場合の処理手段構成を示したブロック図である。

【図４３】本発明の情報記録再生装置において使用される情報記録媒体を製造する製造装置の構成を示すブロック図である。

【図４４】本発明の情報記録再生装置において使用される情報記録媒体を製造する製造処理の処理フローを示す図である。

【図４５】本発明の情報記録再生装置において使用されるキー更新ブロック（ＫＲＢ）のフォーマット例を示す図である。

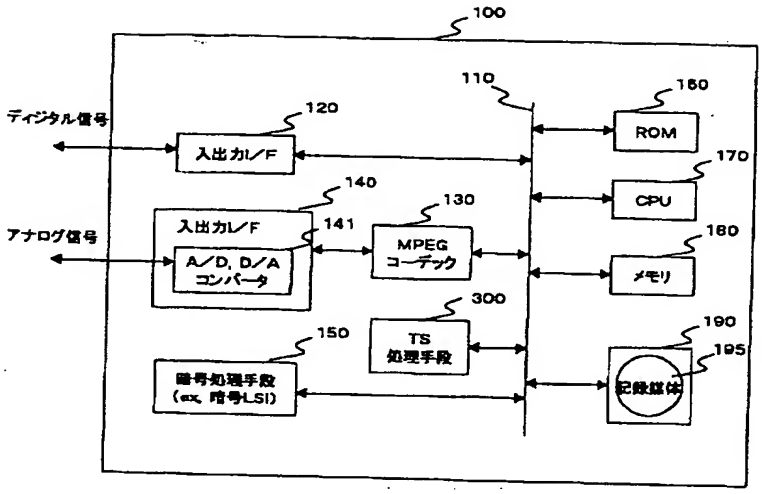
【図４６】本発明の情報記録再生装置において使用されるキー更新ブロック（ＫＲＢ）のタグの構成を説明する図である。

【符号の説明】

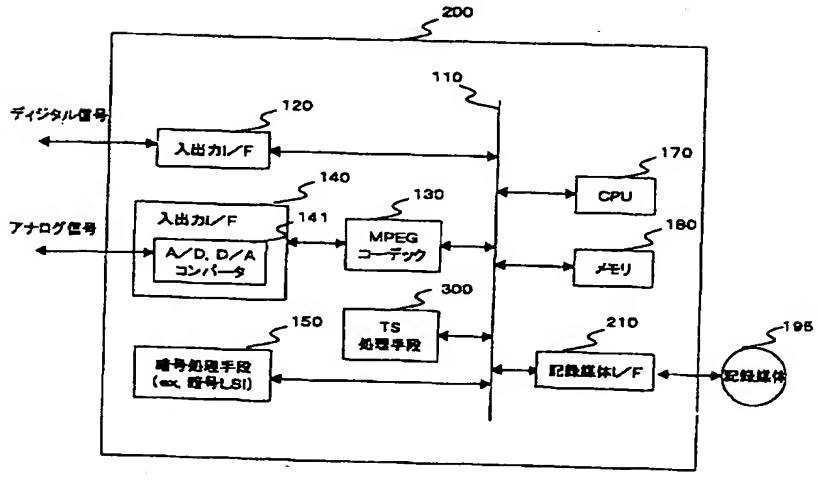
１００，２００　記録再生装置
１１０　バス
１２０　入出力Ｉ／Ｆ
１３０　ＭＰＥＧコーデック
１４０　入出力Ｉ／Ｆ
１４１　Ａ／Ｄ，Ｄ／Ａコンバータ
１５０　暗号処理手段
１６０　ＲＯＭ
１７０　ＣＰＵ
１８０　メモリ
１９０　ドライブ
１９５　記録媒体
２１０　記録媒体Ｉ／Ｆ
３００　ＴＳ処理手段
６００，６０７　端子
６０２　ビットストリームパーサー
６０３　ＰＬＬ
６０４　タイムスタンプ発生回路
６０５　ブロックシード付加回路
６０６　スムージングバッファ
８００，８０６　端子
８０１　ブロックシード分離回路
８０２　出力制御回路
８０３　比較器
８０４　タイミング発生回路
８０５　２７ＭＨｚクロック
９０１，９０４，９１３　端子
９０２　ＭＰＥＧビデオエンコーダ
９０３　ビデオストリームバッファ
９０５　ＭＰＥＧオーディオエンコーダ
９０６　オーディオストリームバッファ
９０８　多重化スケジューラ
９０９　トランスポートパケット符号化器
９１０　到着タイムスタンプ計算手段
９１１　ブロックシード付加回路
９１２　スムージングバッファ
９７６　スイッチ
４２０１　バス
４２０２　ＣＰＵ
４２０３　ＲＯＭ
４２０４　ＲＡＭ
４２０５　ハードディスク
４２０６　出力部
４２０７　入力部
４２０８　通信部
４２０９　ドライブ
４２１０　リムーバブル記録媒体
４２１１　入出力インタフェース
４３００　ディスク製造装置
４３０１　制御部
４３０２　メモリ
４３０３　記録媒体Ｉ／Ｆ
４３０４　入出力Ｉ／Ｆ
４３０５　バス

４３５０　記録媒体
４５０１　バージョン
４５０２　デプス
４５０３　データポインタ
４５０４　タグポインタ
４５０５　署名ポインタ
４５０６　データ部
４５０７　タグ部
４５０８　署名

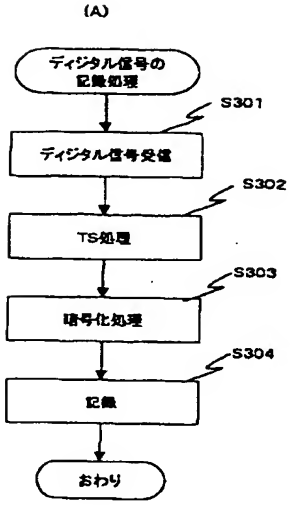
【図１】



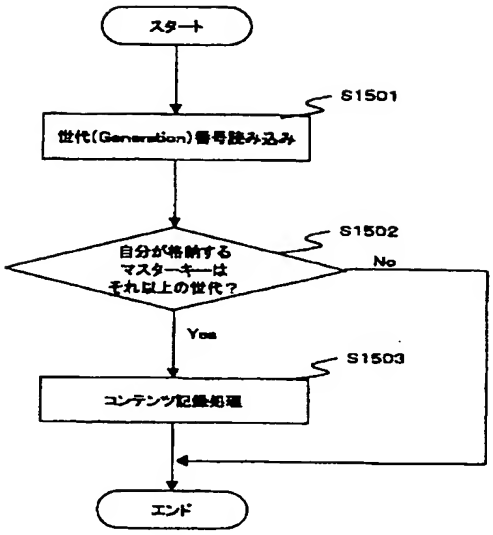
【図２】



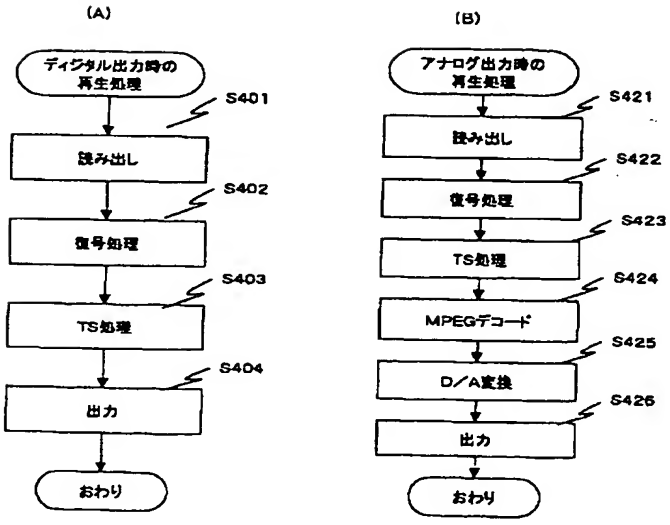
【図３】


(A)
ディジタル信号の記録処理
S301
ディジタル信号受信
S302
TS処理
S303
暗号化処理
S304
記録
おわり
(B)
アナログ信号の記録処理
S321
アナログ信号受信
S322
A／D変換
S323
MPEG符号化
S324
TS処理
S325
暗号化処理
S326
記録
おわり

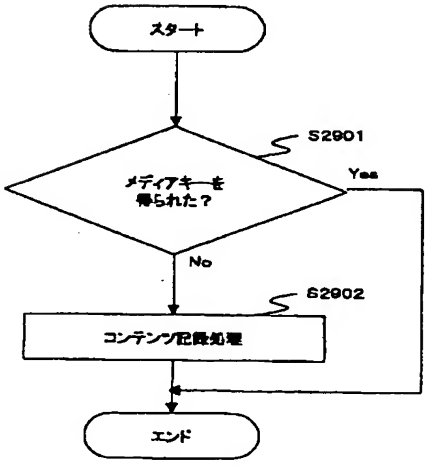
【図１５】


スタート
S1501
世代(Generation)番号読み込み
S1502
自分が格納するマスターキーはそれ以上の世代？
No
Yes
S1503
コンテンツ記録処理
エンド

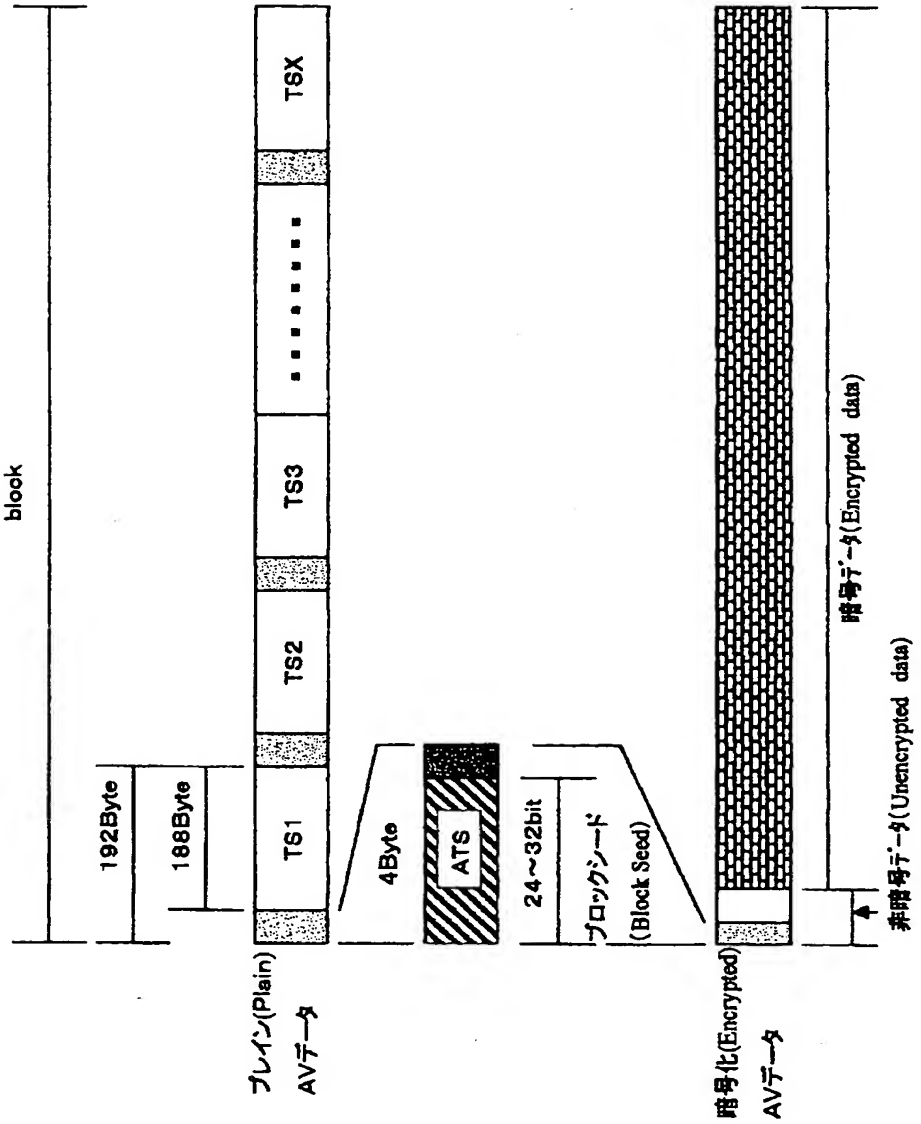
【図４】


(A)
ディジタル出力時の再生処理
S401
読み出し
S402
復号処理
S403
TS処理
S404
出力
おわり
(B)
アナログ出力時の再生処理
S421
読み出し
S422
復号処理
S423
TS処理
S424
MPEGデコード
S425
D／A変換
S426
出力
おわり

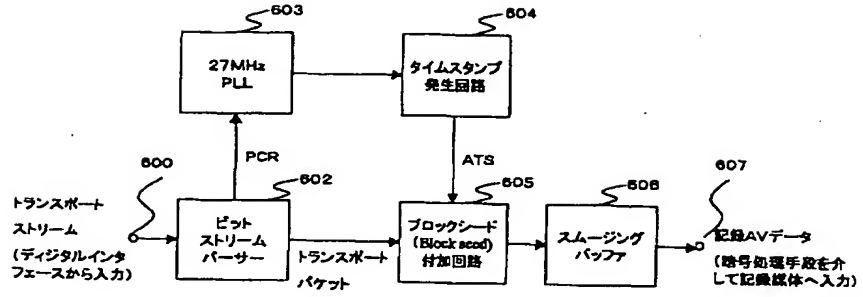
【図２９】


スタート
S2901
メディアキーを得られた？
Yes
No
S2902
コンテンツ記録処理
エンド

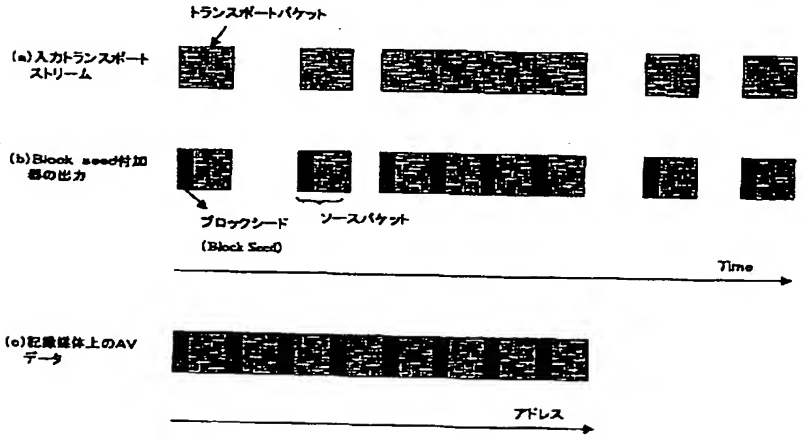
【図５】


block
192Byte
188Byte
TS1
TS2
TS3
TSX
4Byte
ATS
24～32bit
ブロックシード
(Block Seed)
プレイン(Plain)
AVデータ
暗号化(Encrypted)
AVデータ
暗号データ(Encrypted data)
非暗号データ(Unencrypted data)

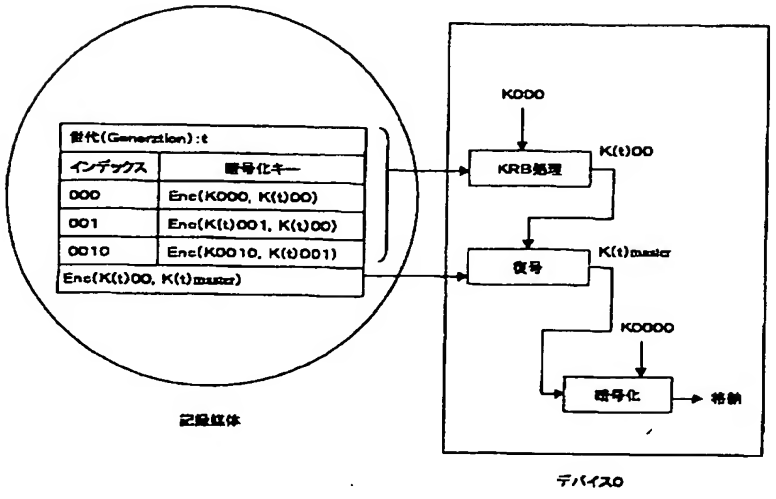
【図６】


603
27MHz
PLL
604
タイムスタンプ
発生回路
PCR
ATS
600
602
605
606
607
トランスポート
ストリーム
（ディジタルインタ
フェースから入力）
ビット
ストリーム
パーサー
トランスポート
パケット
ブロックシード
(Block seed)
付加回路
スムージング
バッファ
記録AVデータ
（暗号処理手段を介
して記録媒体へ入力）

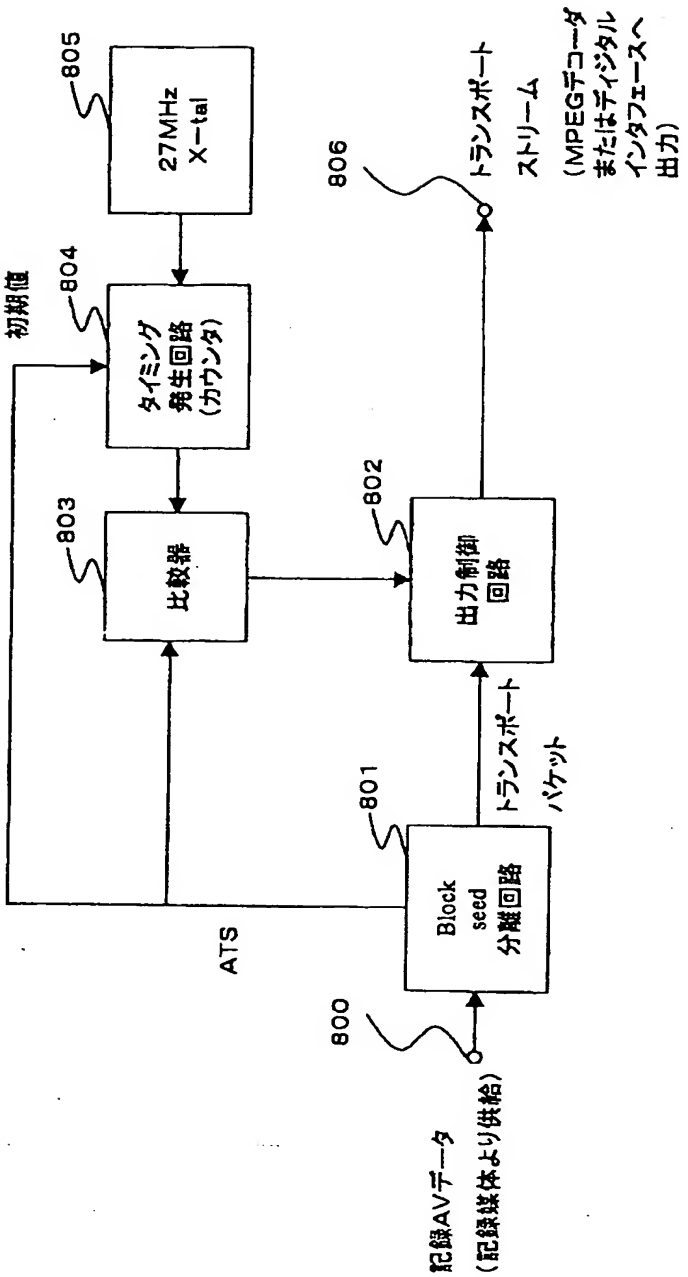
【図７】


トランスポートパケット
(a)入力トランスポート
ストリーム
(b)Block seed付加
器の出力
ブロックシード
(Block Seed)
ソースパケット
Time
(c)記録媒体上のAV
データ
アドレス

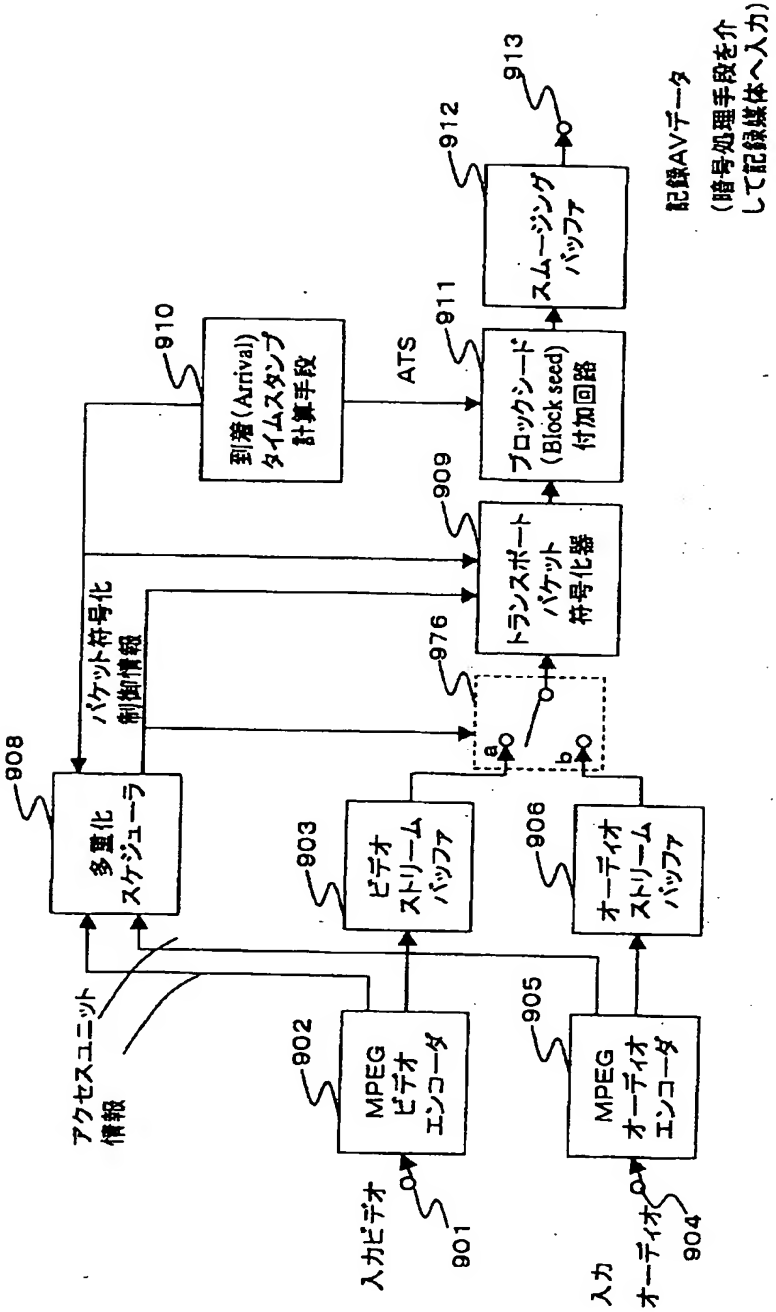
【図１３】


世代(Generation):t
インデックス
暗号化キー
000
Enc(K000, K(t)00)
001
Enc(K(t)001, K(t)00)
0010
Enc(K0010, K(t)001)
Enc(K(t)00, K(t)master)
記録媒体
K000
KRB処理
K(t)00
K(t)master
復号
K0000
暗号化
格納
デバイス0

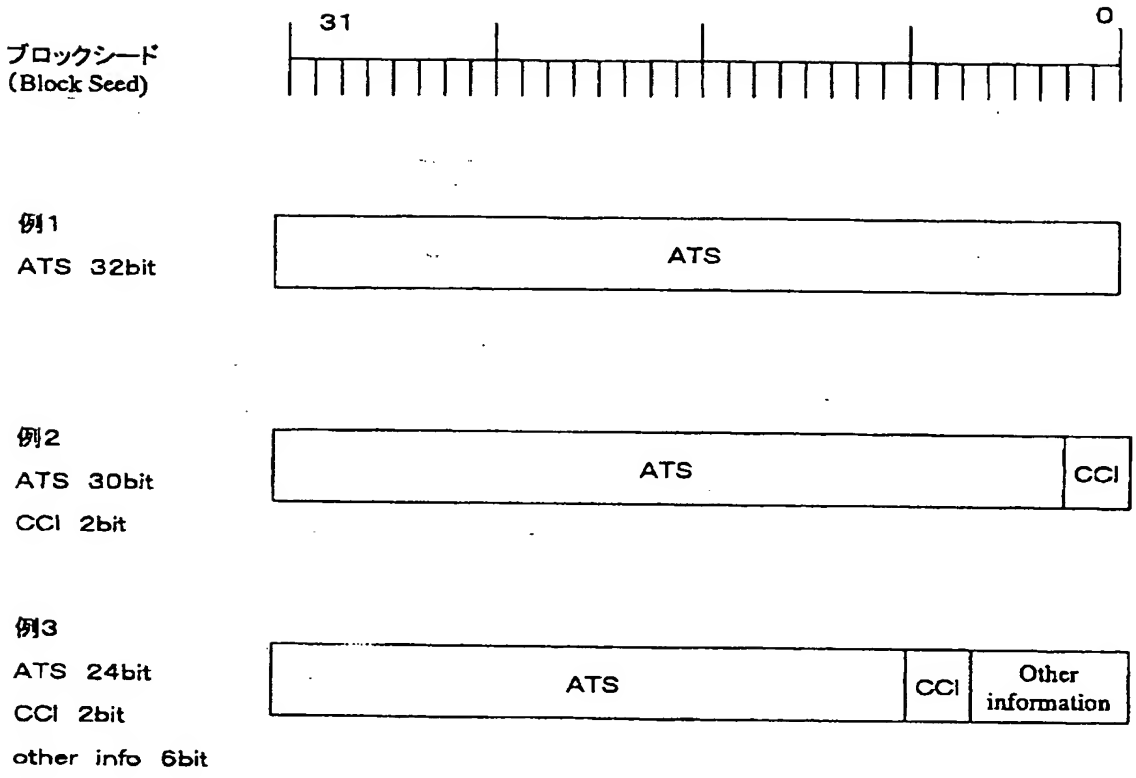
【図８】


805
27MHz
X−tal
806
トランスポート
ストリーム
(MPEGデコーダ
またはディジタル
インタフェースへ
出力)
初期値
804
タイミング
発生回路
(カウンタ)
803
比較器
802
出力制御
回路
801
トランスポート
パケット
Block
seed
分離回路
ATS
800
記録AVデータ
(記録媒体より供給)

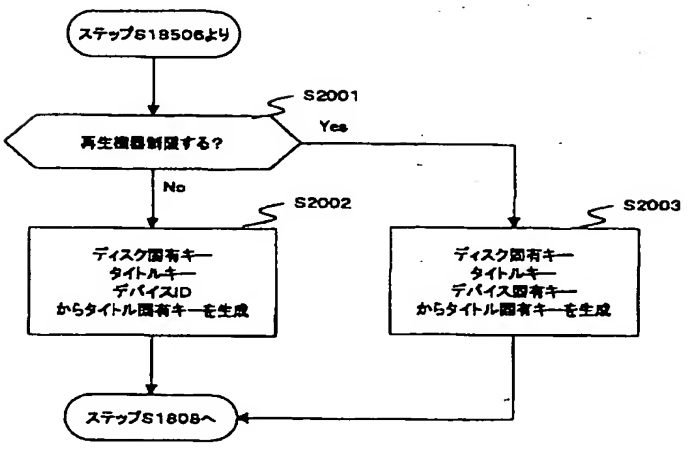
【図９】


入力ビデオ
901
MPEG ビデオ エンコーダ
902
ビデオ ストリーム バッファ
903
入力 オーディオ
904
MPEG オーディオ エンコーダ
905
オーディオ ストリーム バッファ
906
アクセスユニット 情報
多重化 スケジューラ
908
パケット符号化 制御情報
トランスポート パケット 符号化器
909
976
a
b
到着(Arrival) タイムスタンプ 計算手段
910
ATS
ブロックシード (Block seed) 付加回路
911
スムージング バッファ
912
913
記録AVデータ
(暗号処理手段を介して記録媒体へ入力)

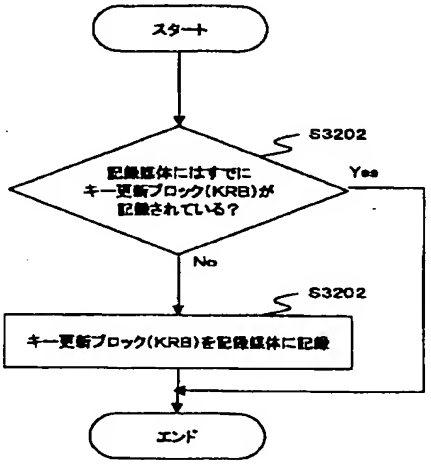
【図10】


31
0
ブロックシード
(Block Seed)
例1
ATS 32bit
ATS
例2
ATS 30bit
CCI 2bit
ATS
CCI
例3
ATS 24bit
CCI 2bit
other info 6bit
ATS
CCI
Other information

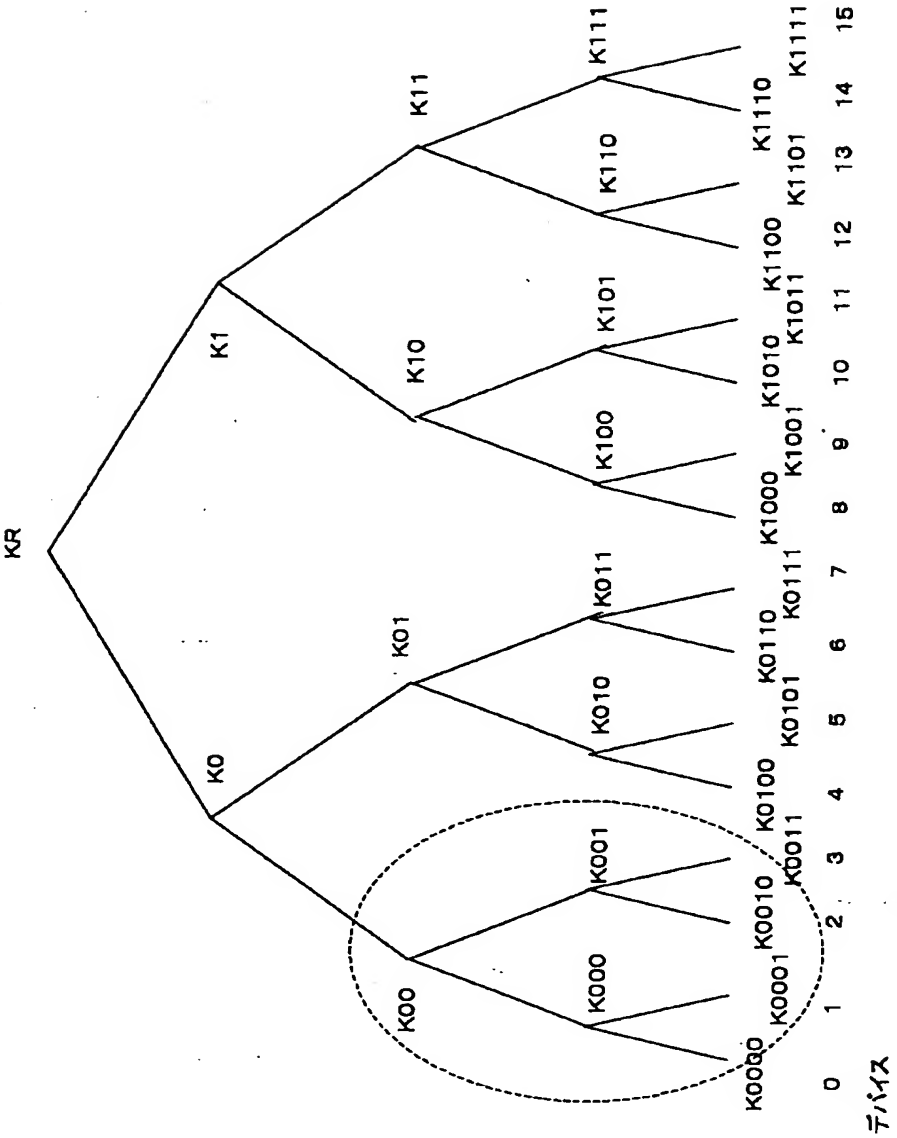
【図20】


ステップS18506より
S2001
再生機器制限する?
Yes
No
S2002
ディスク固有キー
タイトルキー
デバイスID
からタイトル固有キーを生成
S2003
ディスク固有キー
タイトルキー
デバイス固有キー
からタイトル固有キーを生成
ステップS1808へ

【図38】


スタート
S3202
記録媒体にはすでに
キー更新ブロック(KRB)が
記録されている?
Yes
No
S3202
キー更新ブロック(KRB)を記録媒体に記録
エンド

【図１１】


KR
K0
K1
K00
K01
K10
K11
K000
K001
K010
K011
K100
K101
K110
K111
K0000
K0001
K0010
K0011
K0100
K0101
K0110
K0111
K1000
K1001
K1010
K1011
K1100
K1101
K1110
K1111
0
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
デバイス

【図１２】

(A) キー更新ブロック(KRB:Key Renewal Block) 例1

デバイス0, 1, 2にt時点でのルートキーK(t)Rを送付

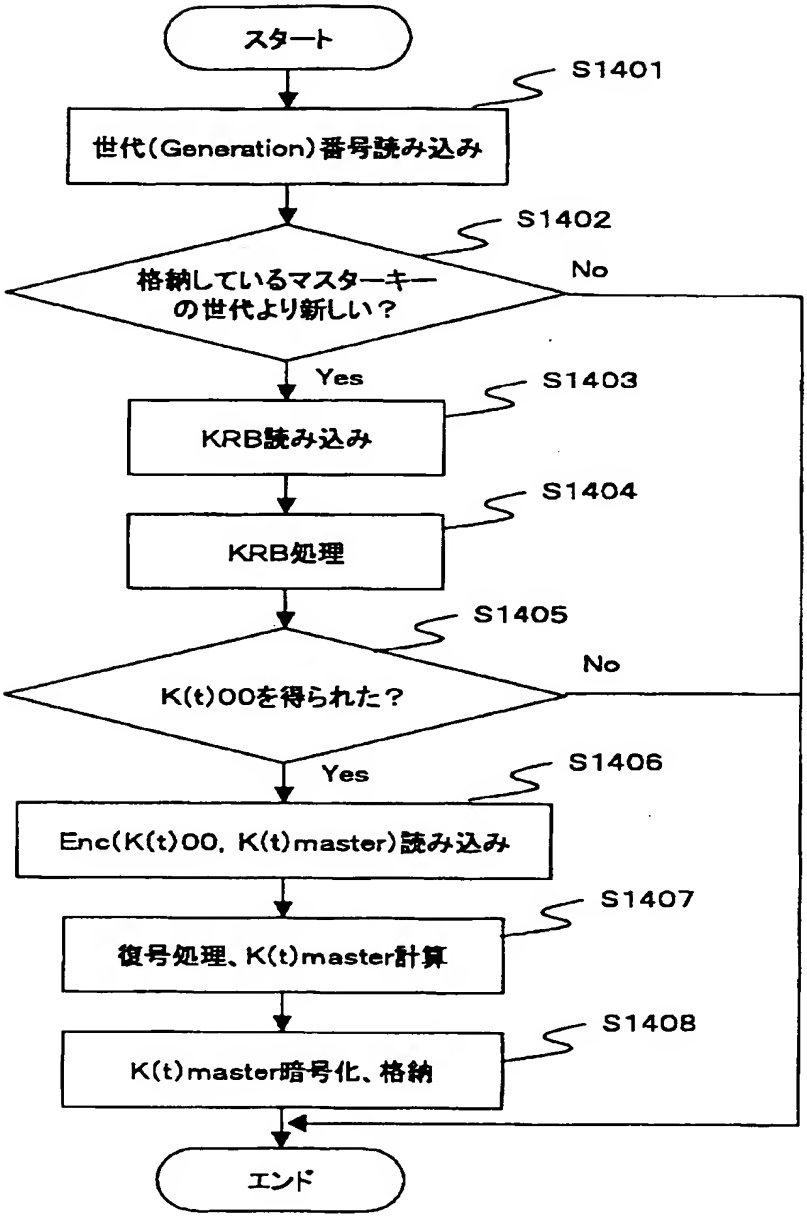
世代(Generztion):t	
インデックス	暗号化キー
0	Enc(K(t)0, K(t)R)
00	Enc(K(t)00, K(t)0)
000	Enc(K000, K(t)00)
001	Enc(K(t)001, K(t)00)
0010	Enc(K0010, K(t)001)

(B) キー更新ブロック(KRB:Key Renewal Block) 例2

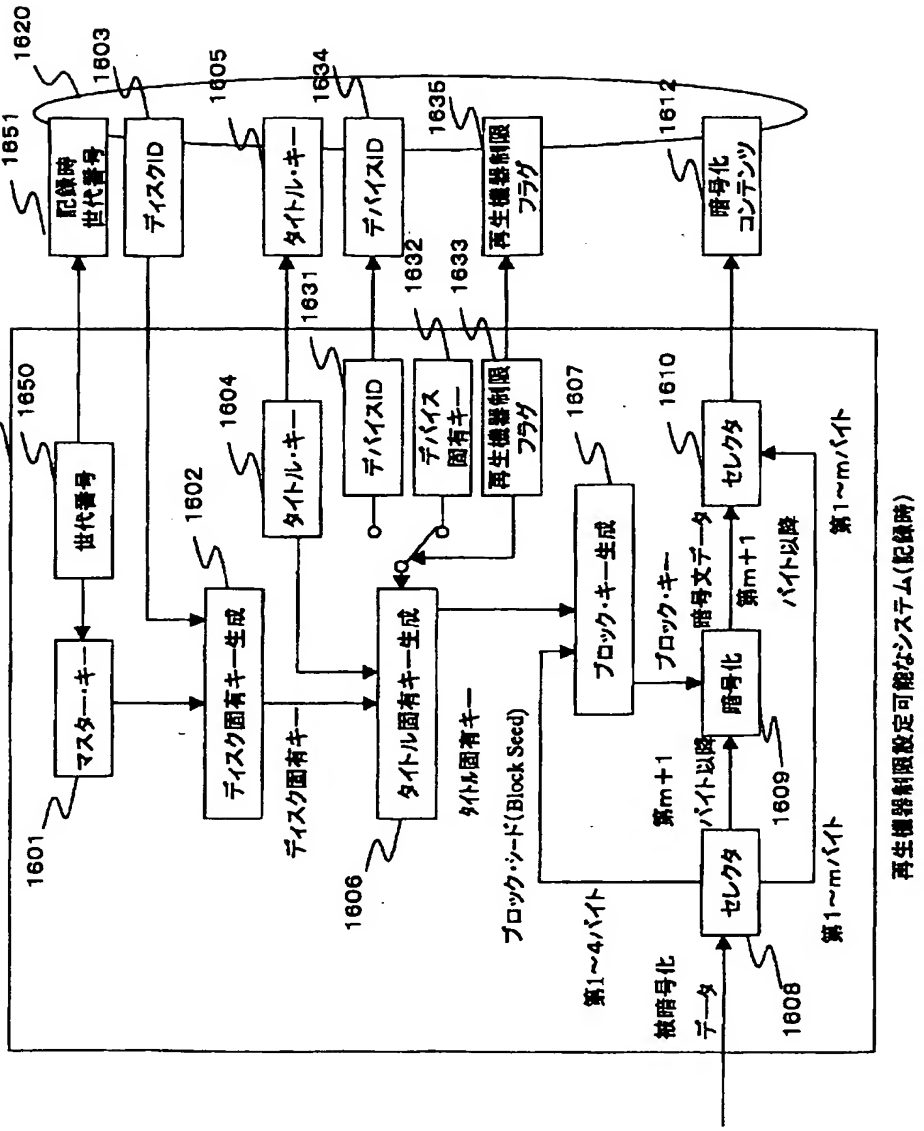
デバイス0, 1, 2にt時点でのルートキーK(t)Rを送付

世代(Generztion):t	
インデックス	暗号化キー
000	Enc(K000, K(t)00)
001	Enc(K(t)001, K(t)00)
0010	Enc(K0010, K(t)001)

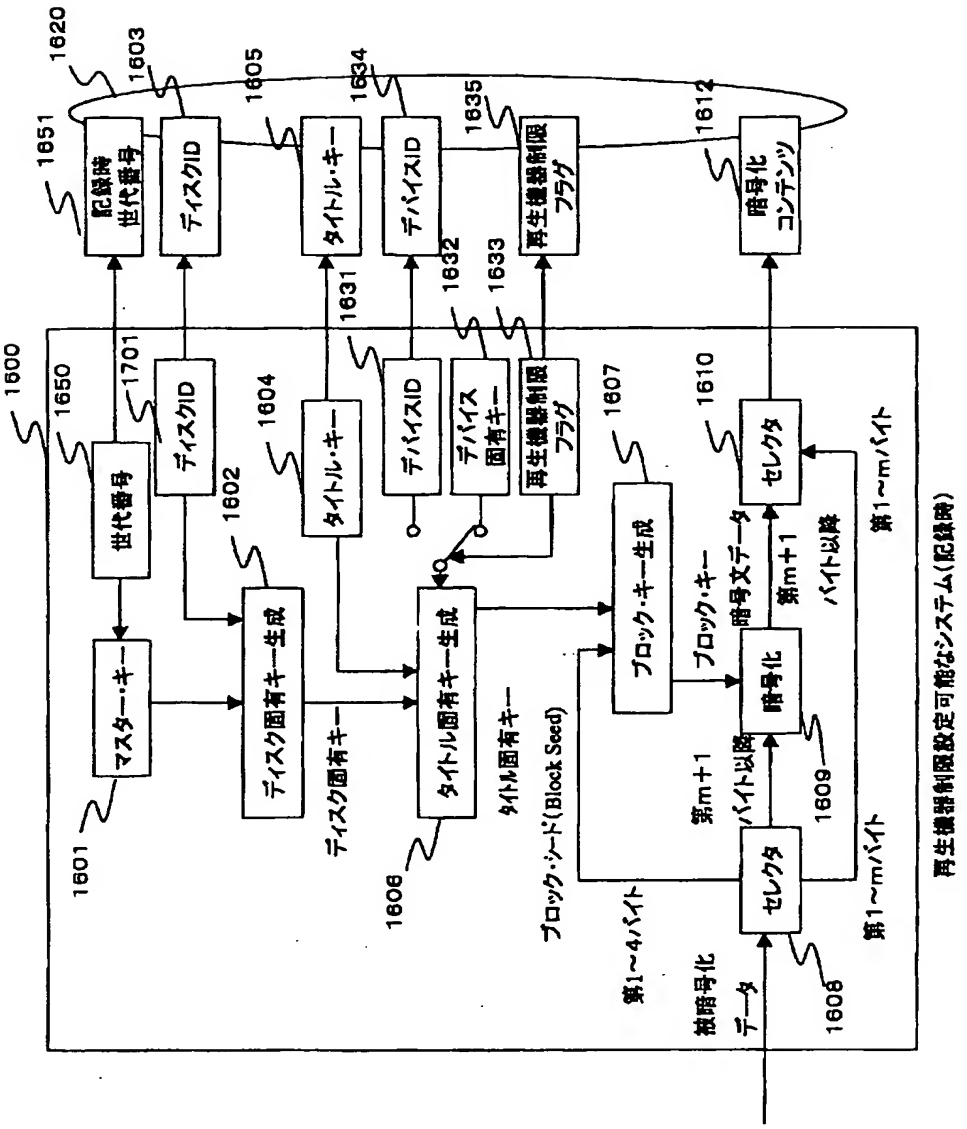
【図１４】


スタート
S1401
世代(Generation)番号読み込み
S1402
格納しているマスターキーの世代より新しい？
No
Yes
S1403
KRB読み込み
S1404
KRB処理
S1405
K(t)00を得られた？
No
Yes
S1406
Enc(K(t)00, K(t)master)読み込み
S1407
復号処理、K(t)master計算
S1408
K(t)master暗号化、格納
エンド

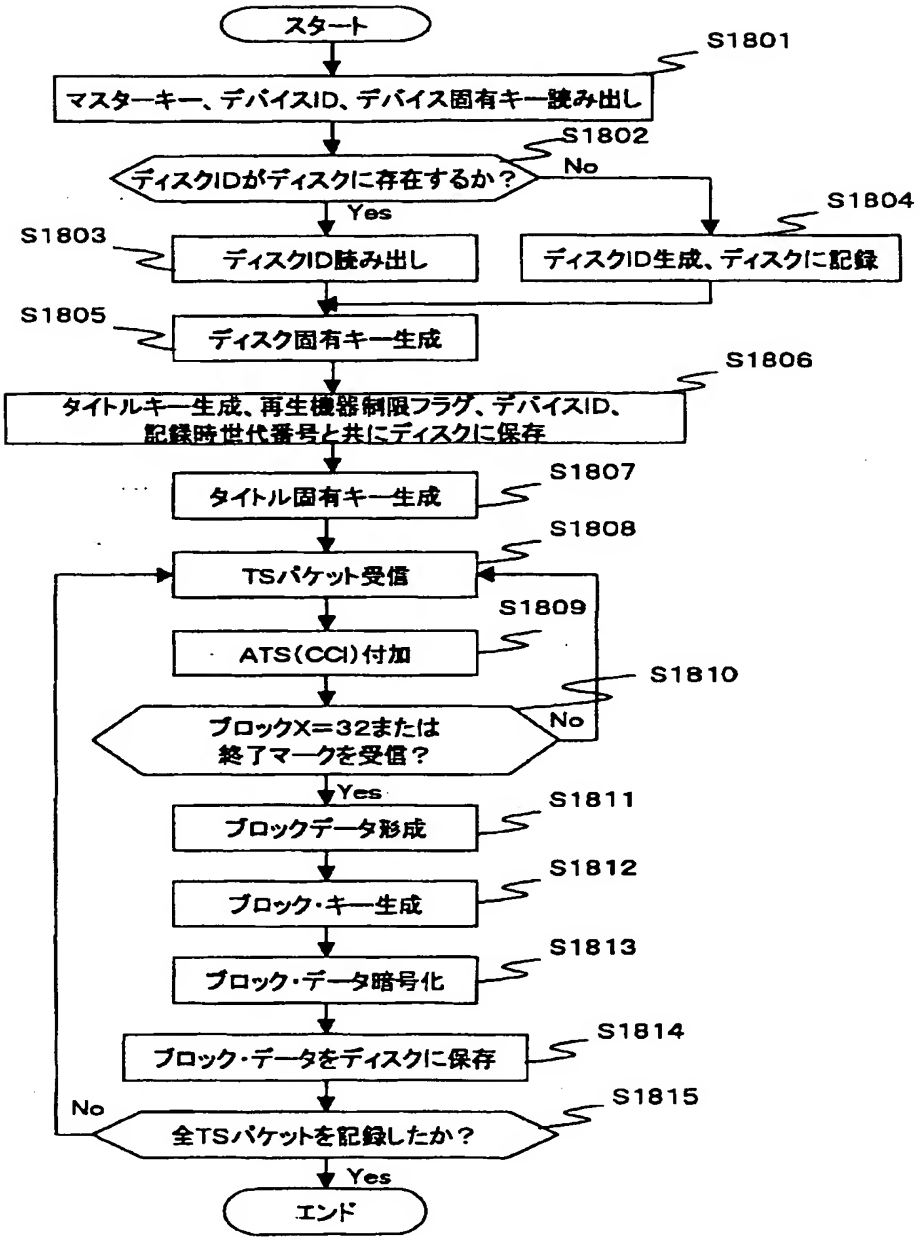
【図１６】


1620
1603
1605
1634
1635
1612
1651
記録時世代番号
ディスクID
タイトル・キー
デバイスID
再生機器制限フラグ
暗号化コンテンツ
1632
1633
1631
1600
1650
1604
1607
1610
世代番号
タイトル・キー
デバイスID
デバイス固有キー
再生機器制限フラグ
セレクタ
1602
マスター・キー
ディスク固有キー生成
タイトル固有キー生成
ブロック・キー生成
ブロック・キー
暗号文データ
第m＋1
バイト以降
第1～mバイト
1601
ディスク固有キー
1606
タイトル固有キー
ブロック・シード(Block Seed)
暗号化
1609
第m＋1
バイト以降
第1～4バイト
セレクタ
被暗号化
データ
1608
第1～mバイト
再生機器制限設定可能なシステム(記録時)

【図１７】


1620
1603
1605
1634
1635
1612
1651
記録時世代番号
ディスクID
タイトル・キー
デバイスID
再生機器制限フラグ
暗号化コンテンツ
1600
1650
1701
1631
1632
1633
1604
1607
1610
世代番号
ディスクID
タイトル・キー
デバイスID
デバイス固有キー
再生機器制限フラグ
セレクタ
1602
マスター・キー
ディスク固有キー生成
タイトル固有キー生成
ブロック・キー生成
暗号化
1601
ディスク固有キー
1606
タイトル固有キー
ブロック・キー
暗号文データ
第m＋1バイト以降
第1～mバイト
ブロック・シード(Block Seed)
第m＋1バイト以降
1609
第1～4バイト
被暗号化データ
セレクタ
1608
第1～mバイト
再生機器制限設定可能なシステム(記録時)

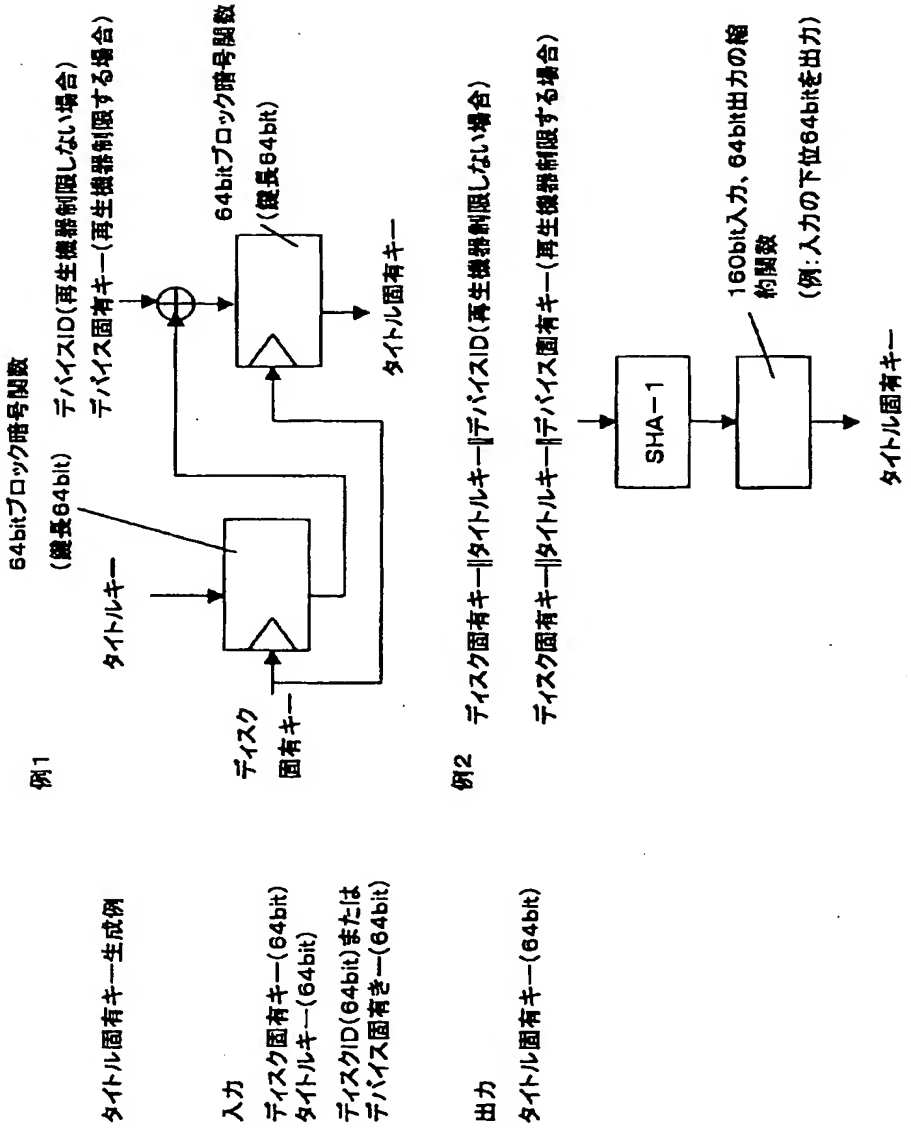
【図１８】


スタート
S1801
マスターキー、デバイスID、デバイス固有キー読み出し
S1802
ディスクIDがディスクに存在するか？
No
Yes
S1803
ディスクID読み出し
S1804
ディスクID生成、ディスクに記録
S1805
ディスク固有キー生成
S1806
タイトルキー生成、再生機器制限フラグ、デバイスID、
記録時世代番号と共にディスクに保存
S1807
タイトル固有キー生成
S1808
TSパケット受信
S1809
ATS(CCI)付加
S1810
ブロックX＝32または
終了マークを受信？
No
Yes
S1811
ブロックデータ形成
S1812
ブロック・キー生成
S1813
ブロック・データ暗号化
S1814
ブロック・データをディスクに保存
S1815
No
全TSパケットを記録したか？
Yes
エンド

【図１９】

例1
ディスク固有キー生成例
入力
マスターキー(64bit)
ディスクID(64bit)
出力
ディスク固有キー(64bit)
ディスクID(64bit)
64bitブロック暗号関数
(鍵長64bit)
マスターキー
ディスク固有キー
例2
マスターキー‖ディスクID
SHA－1
160bit入力、64bit出力の縮約関数
(例:入力の下位64bitを出力)
ディスク固有キー

【図２１】


タイトル固有キー生成例
入力
ディスク固有キー(64bit)
タイトルキー(64bit)
ディスクID(64bit)またはデバイス固有キー(64bit)
出力
タイトル固有キー(64bit)
例1
64bitブロック暗号関数
(鍵長64bit)
タイトルキー
ディスク固有キー
デバイスID(再生機器制限しない場合)
デバイス固有キー(再生機器制限する場合)
64bitブロック暗号関数
(鍵長64bit)
タイトル固有キー
例2
ディスク固有キー‖タイトルキー‖デバイスID(再生機器制限しない場合)
ディスク固有キー‖タイトルキー‖デバイス固有キー(再生機器制限する場合)
SHA－1
160bit入力、64bit出力の縮約関数
(例:入力の下位64bitを出力)
タイトル固有キー

【図22】

例1

ブロック・キー生成例

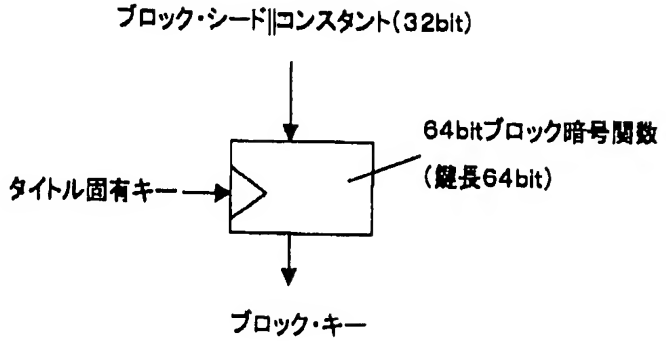
入力

ブロック・シード(32bit)

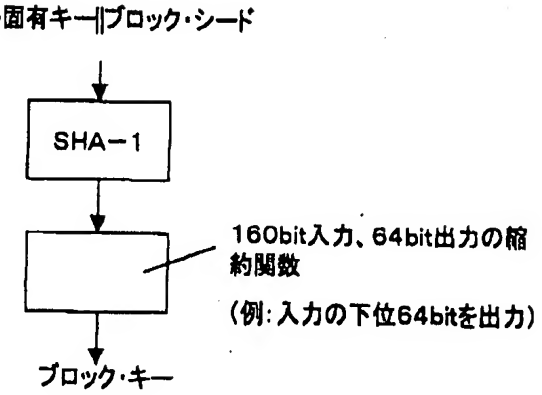
タイトル固有キー(64bit)

出力

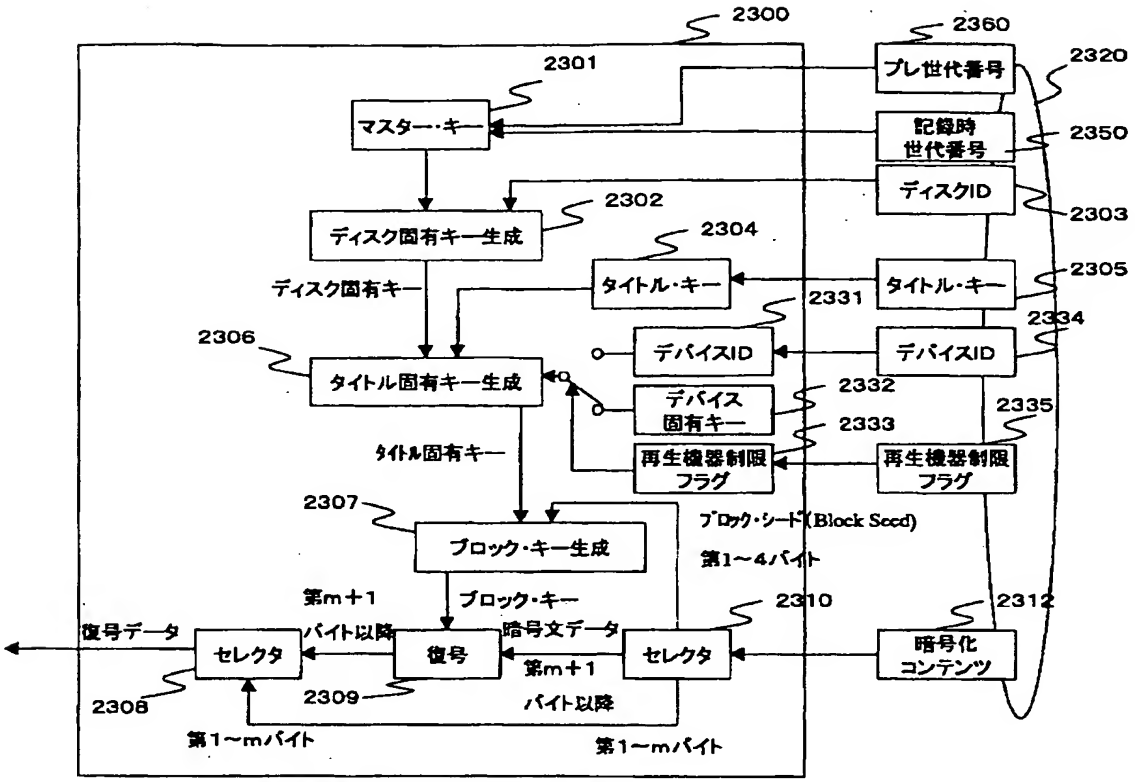
ブロック・キー(64bit)



例2

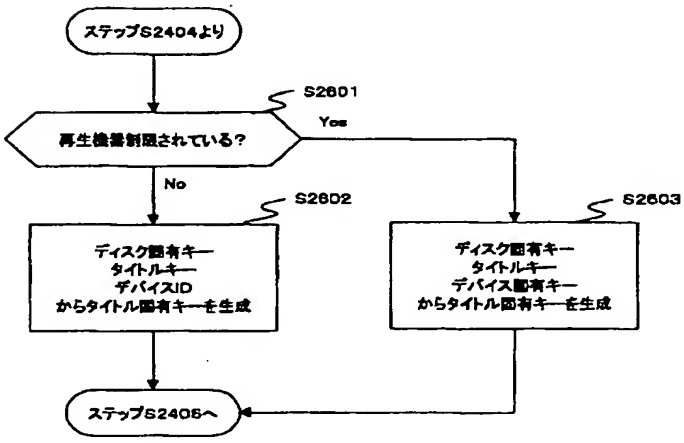


【図２３】

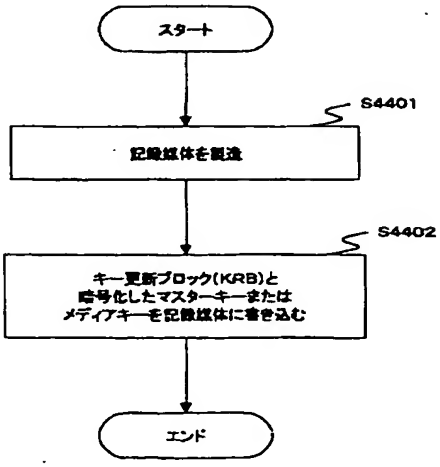


再生機器制限設定可能なシステム(再生時)

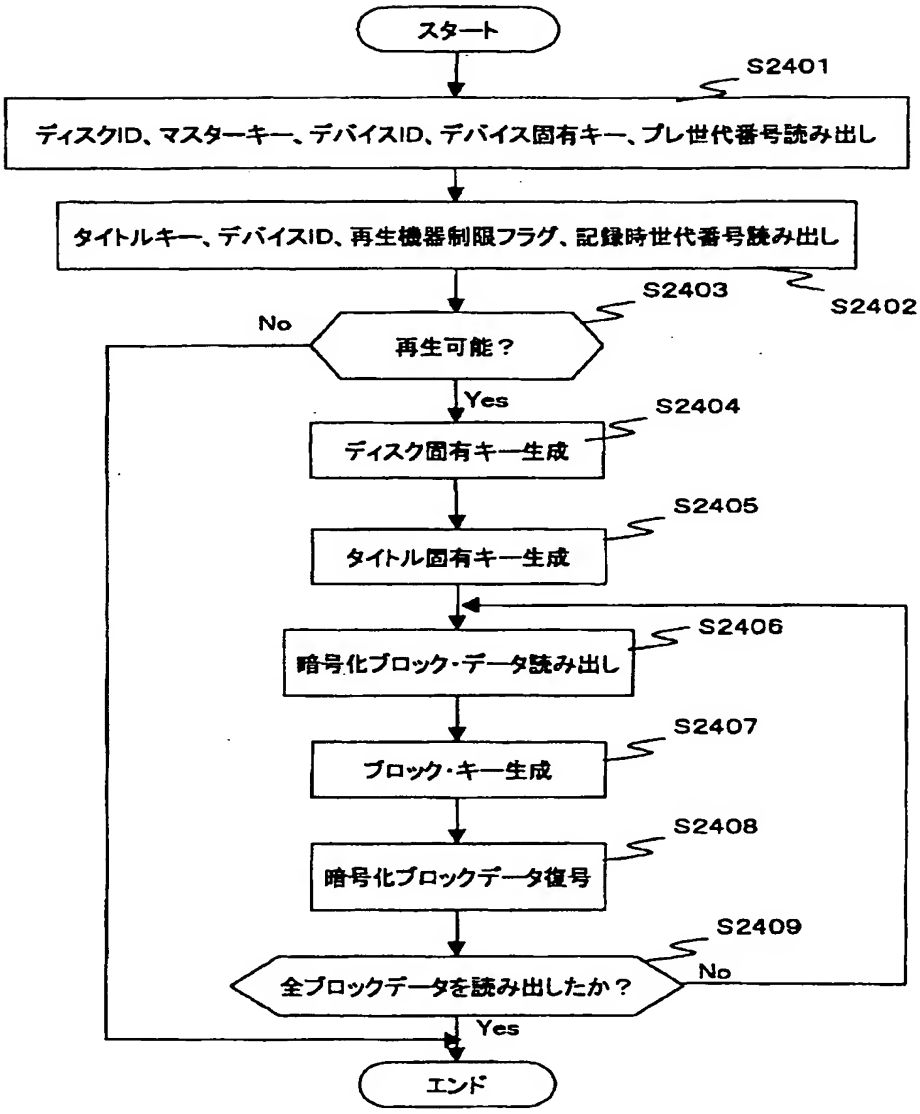
【図２６】



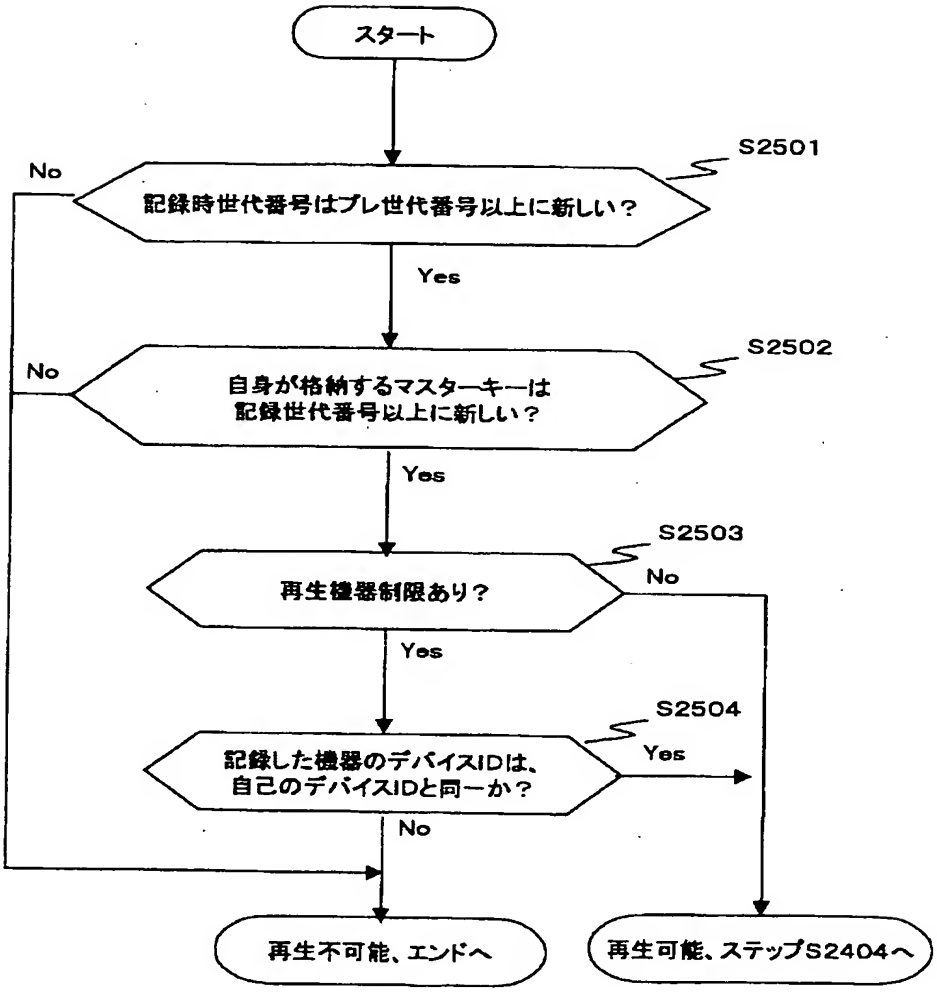
【図４４】



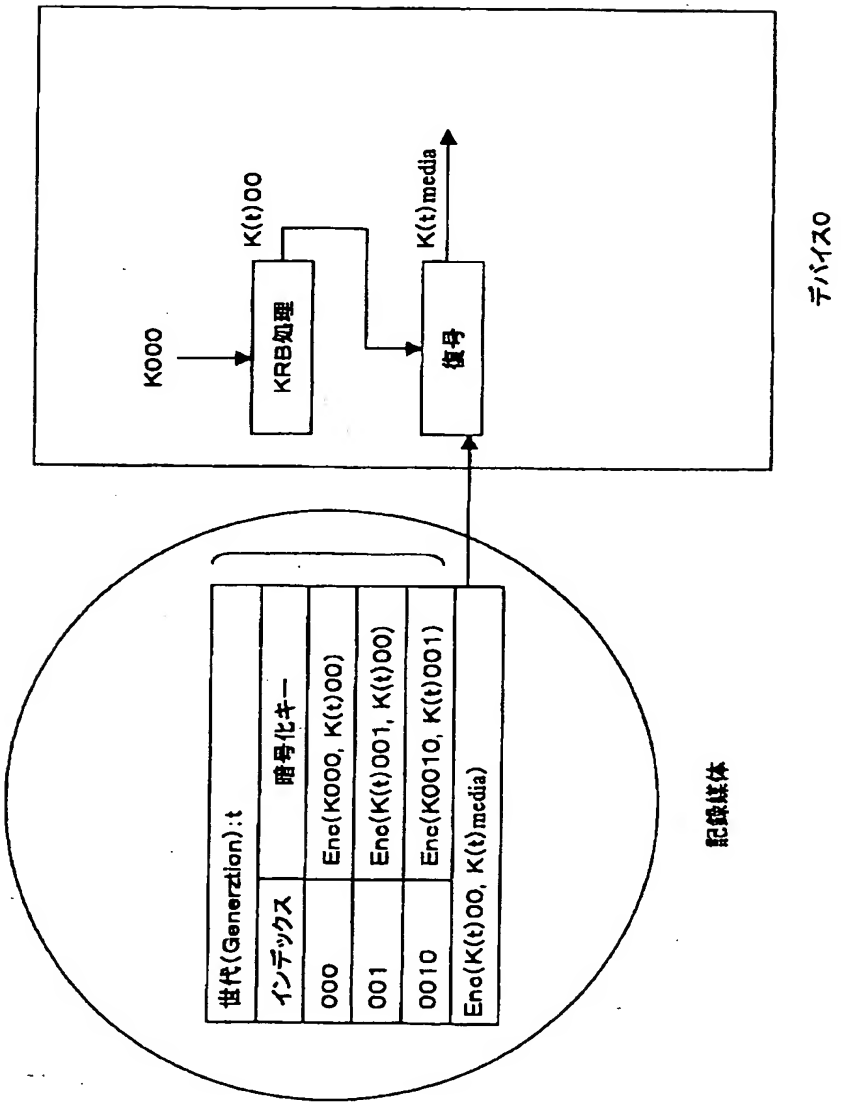
【図２４】


スタート
S2401
ディスクID、マスターキー、デバイスID、デバイス固有キー、プレ世代番号読み出し
タイトルキー、デバイスID、再生機器制限フラグ、記録時世代番号読み出し
S2402
S2403
No
再生可能？
Yes
S2404
ディスク固有キー生成
S2405
タイトル固有キー生成
S2406
暗号化ブロック・データ読み出し
S2407
ブロック・キー生成
S2408
暗号化ブロックデータ復号
S2409
全ブロックデータを読み出したか？
No
Yes
エンド

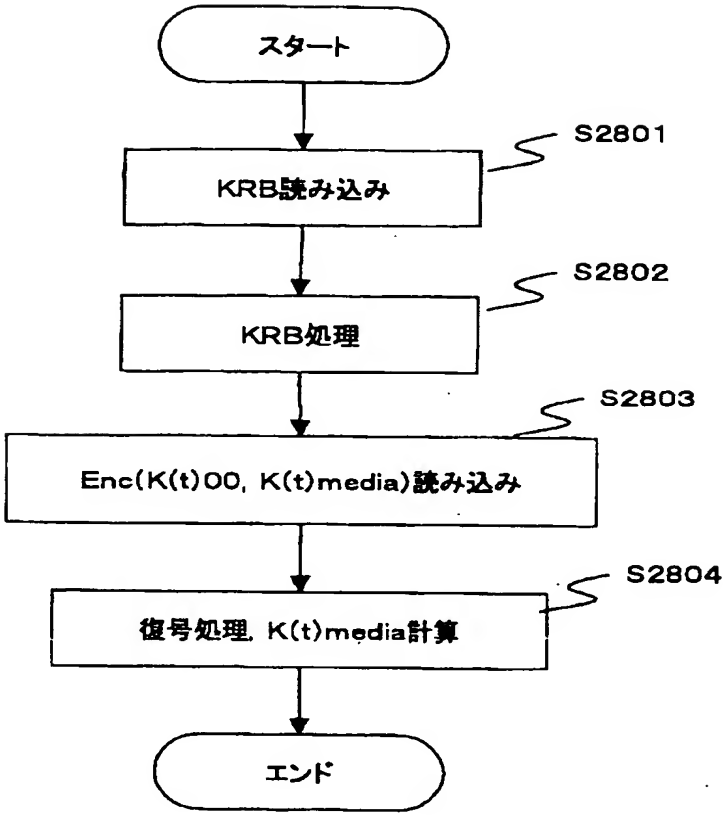
【図２５】


スタート
S2501
No
記録時世代番号はプレ世代番号以上に新しい？
Yes
S2502
No
自身が格納するマスターキーは
記録世代番号以上に新しい？
Yes
S2503
再生機器制限あり？
No
Yes
S2504
記録した機器のデバイスIDは、
自己のデバイスIDと同一か？
Yes
No
再生不可能、エンドへ
再生可能、ステップS2404へ

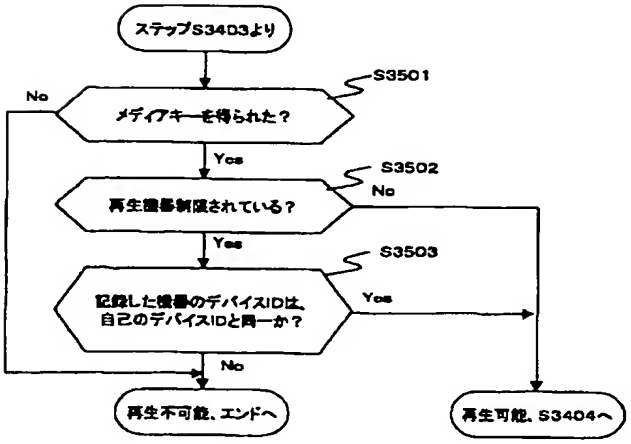
【図２７】


K000
KRB処理
K(t)00
復号
K(t)media
デバイス0
世代(Generation):t
インデックス
暗号化キー
000
Enc(K000, K(t)00)
001
Enc(K(t)001, K(t)00)
0010
Enc(K0010, K(t)001)
Enc(K(t)00, K(t)media)
記録媒体

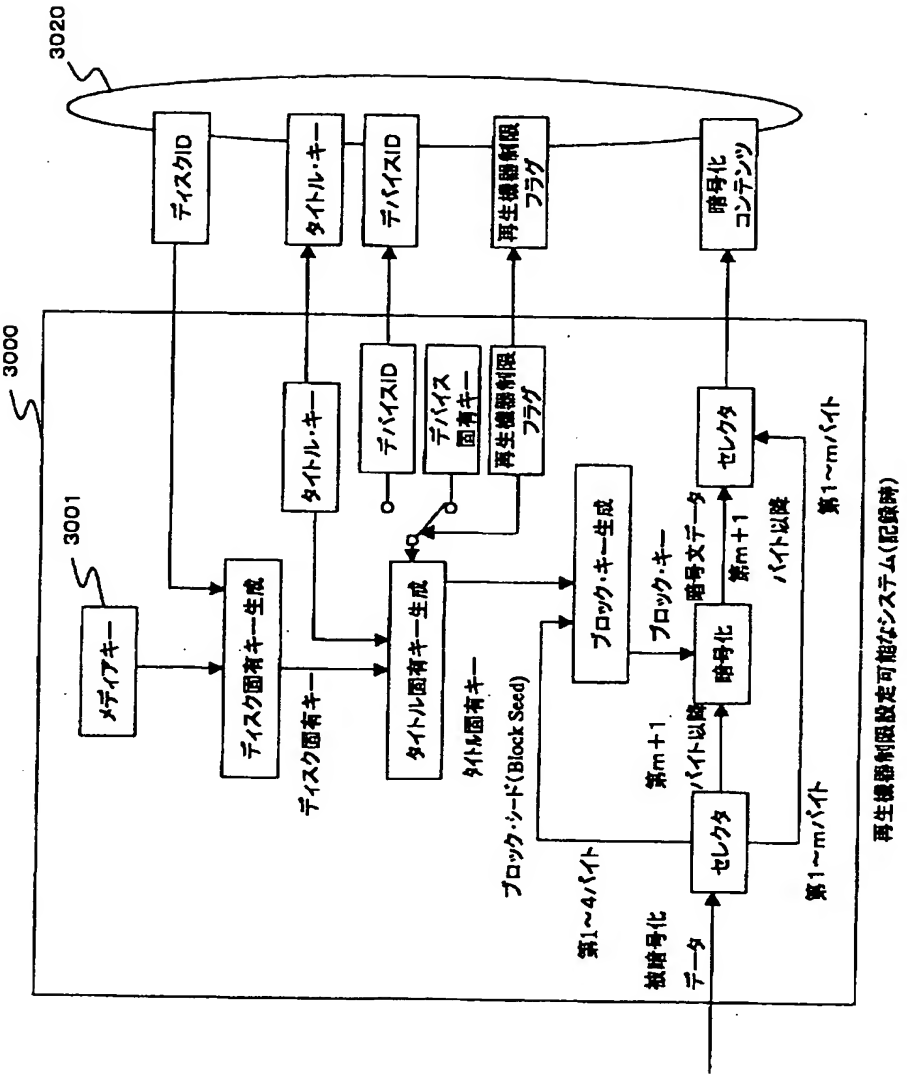
【図２８】


スタート
S2801
KRB読み込み
S2802
KRB処理
S2803
Enc(K(t)00, K(t)media)読み込み
S2804
復号処理, K(t)media計算
エンド

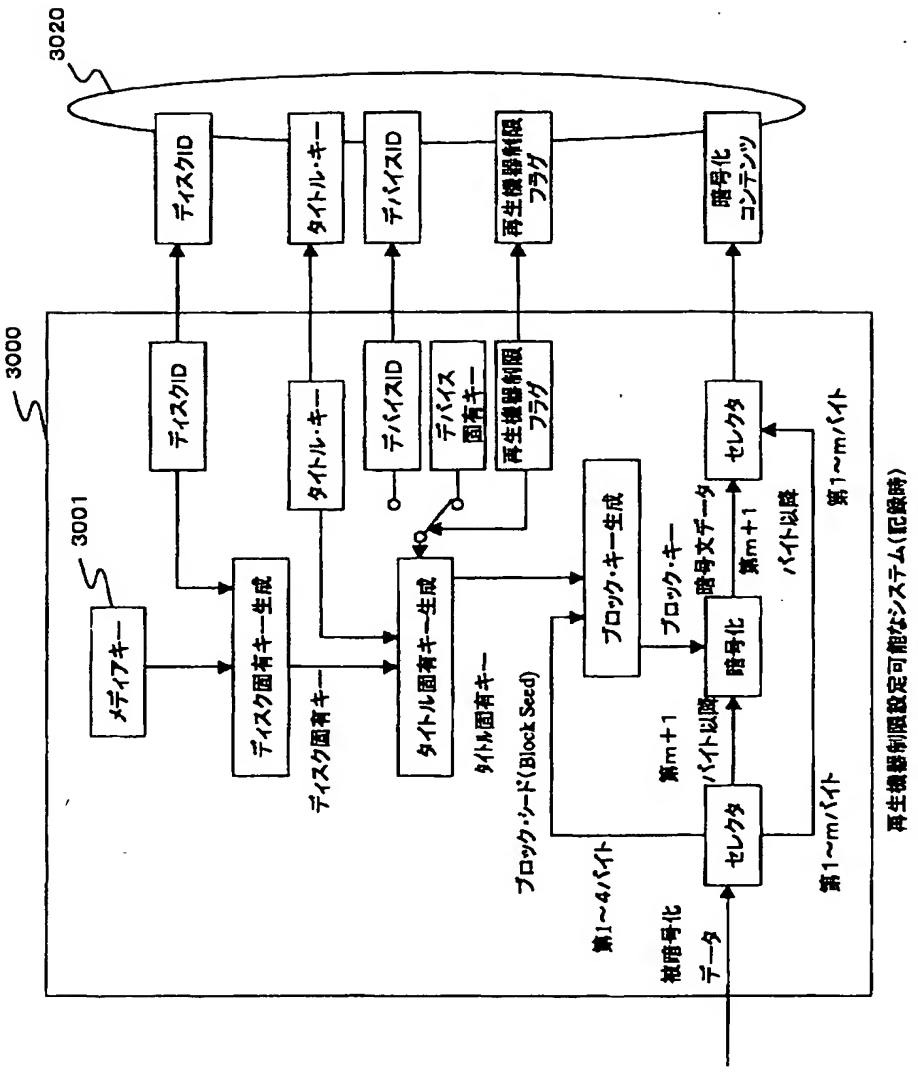
【図３５】


ステップS3403より
S3501
No
メディアキーを得られた？
Yes
S3502
再生回数制限されている？
No
Yes
S3503
記録した機器のデバイスIDは、
自己のデバイスIDと同一か？
Yes
No
再生不可能、エンドへ
再生可能、S3404へ

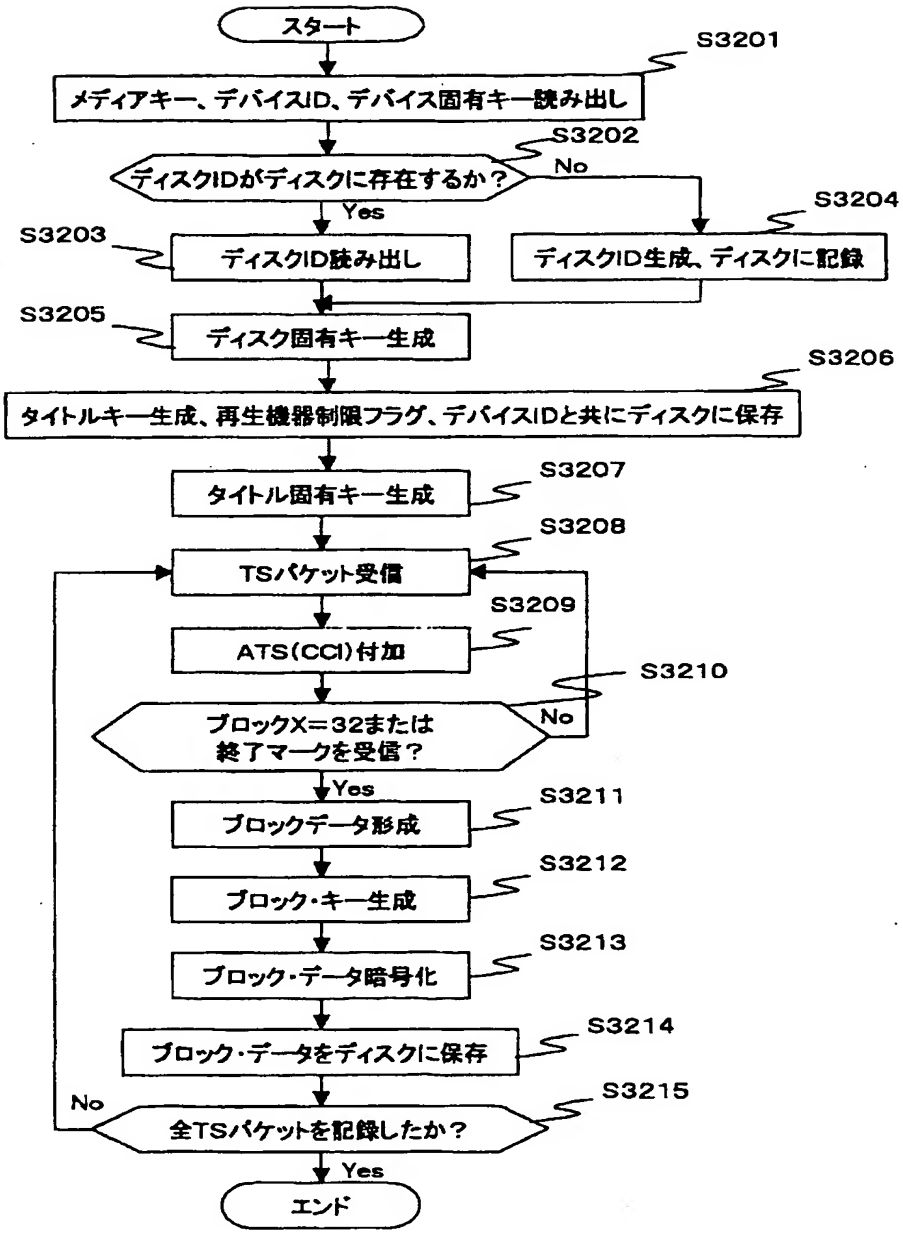
【図３０】


3020
ディスクID
タイトル・キー
デバイスID
再生機器制限フラグ
暗号化コンテンツ
3000
3001
メディアキー
ディスク固有キー生成
ディスク固有キー
タイトル・キー
デバイスID
デバイス固有キー
再生機器制限フラグ
タイトル固有キー生成
タイトル固有キー
ブロック・シード(Block Seed)
ブロック・キー生成
ブロック・キー
暗号文データ
暗号化
セレクタ
第m+1バイト以降
第1～mバイト
第1～4バイト
第m+1バイト以降
第1～mバイト
被暗号化データ
再生機器制限設定可能なシステム(記録時)

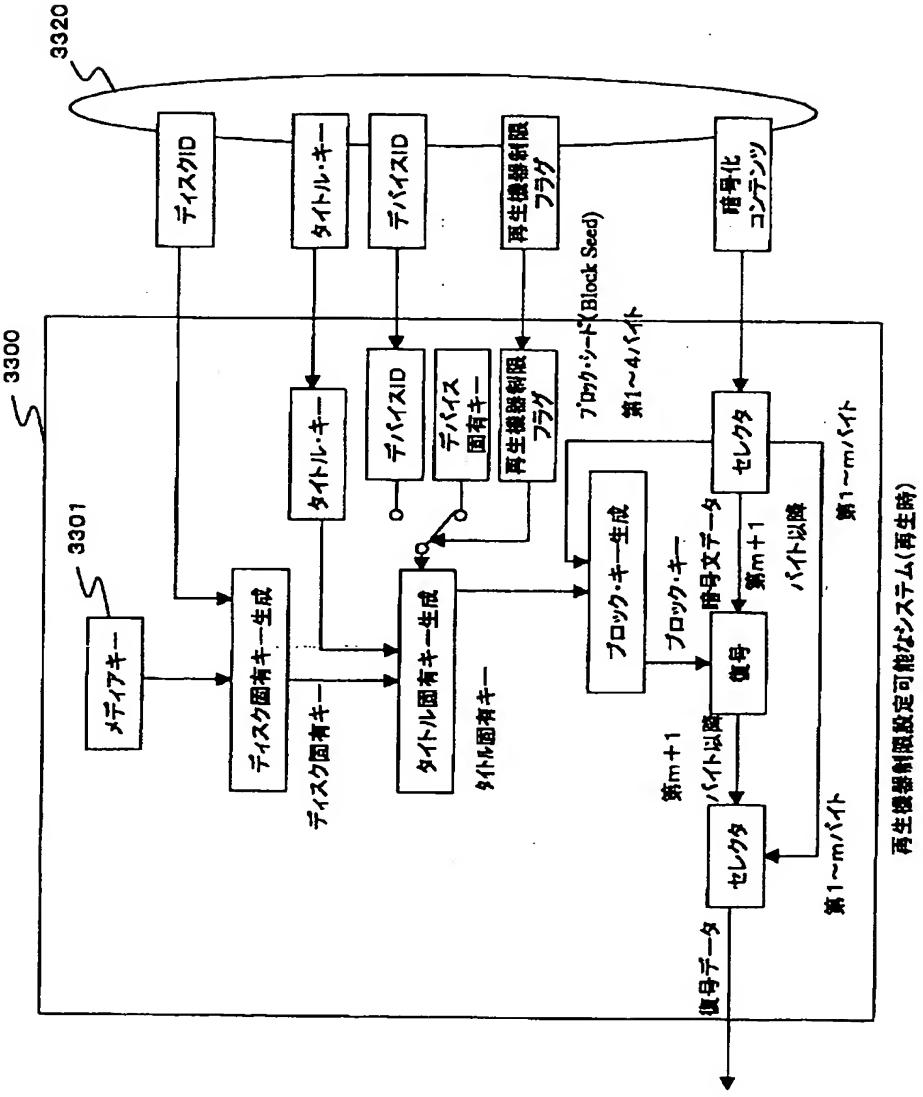
【図３１】


3020
ディスクID
タイトル・キー
デバイスID
再生機器制限フラグ
暗号化コンテンツ
3000
3001
メディアキー
ディスク固有キー生成
タイトル固有キー生成
ブロック・キー生成
セレクタ
暗号化
ディスクID
タイトル・キー
デバイスID
デバイス固有キー
再生機器制限フラグ
ディスク固有キー
タイトル固有キー
ブロック・シード(Block Seed)
ブロック・キー
暗号文データ
第m＋1バイト以降
第1～mバイト
第1～4バイト
第m＋1バイト以降
第1～mバイト
被暗号化データ
再生機器制限設定可能なシステム(記録時)

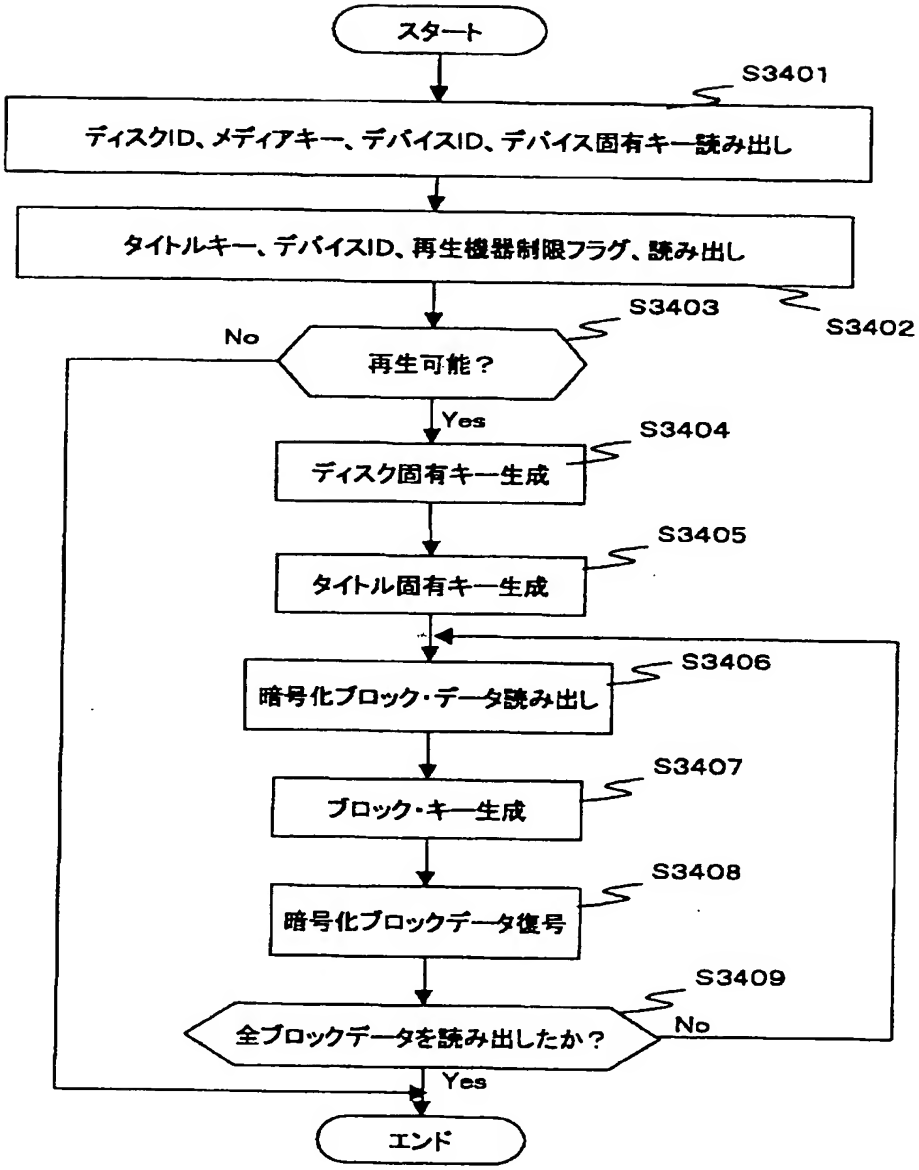
【図３２】


スタート
S3201
メディアキー、デバイスID、デバイス固有キー読み出し
S3202
ディスクIDがディスクに存在するか？
No
Yes
S3203
ディスクID読み出し
S3204
ディスクID生成、ディスクに記録
S3205
ディスク固有キー生成
S3206
タイトルキー生成、再生機器制限フラグ、デバイスIDと共にディスクに保存
S3207
タイトル固有キー生成
S3208
TSパケット受信
S3209
ATS(CCI)付加
S3210
ブロックX＝32または
終了マークを受信？
No
Yes
S3211
ブロックデータ形成
S3212
ブロック・キー生成
S3213
ブロック・データ暗号化
S3214
ブロック・データをディスクに保存
S3215
No
全TSパケットを記録したか？
Yes
エンド

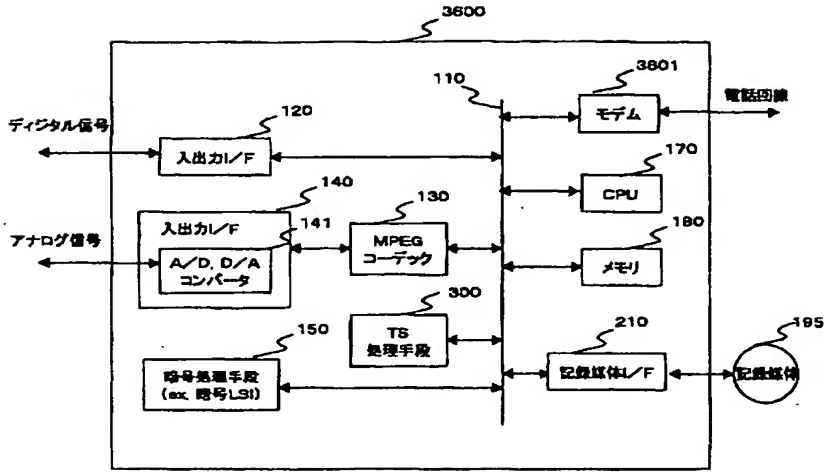
【図３３】


3320
ディスクID
タイトル・キー
デバイスID
再生機器制限フラグ
暗号化コンテンツ
3300
3301
メディアキー
ディスク固有キー生成
ディスク固有キー
タイトル・キー
デバイスID
デバイス固有キー
再生機器制限フラグ
タイトル固有キー生成
タイトル固有キー
ブロック・シード(Block Seed)
第1~4バイト
ブロック・キー生成
ブロック・キー
セレクタ
暗号文データ
第m+1
バイト以降
第1~mバイト
復号
第m+1
バイト以降
セレクタ
第1~mバイト
復号データ
再生機器制限設定可能なシステム(再生時)

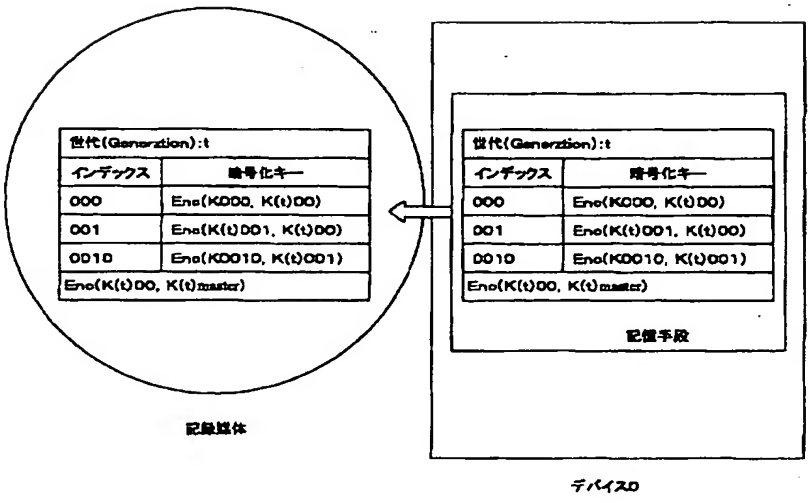
【図３４】


スタート
S3401
ディスクID、メディアキー、デバイスID、デバイス固有キー読み出し
タイトルキー、デバイスID、再生機器制限フラグ、読み出し
S3402
S3403
No
再生可能？
Yes
S3404
ディスク固有キー生成
S3405
タイトル固有キー生成
S3406
暗号化ブロック・データ読み出し
S3407
ブロック・キー生成
S3408
暗号化ブロックデータ復号
S3409
全ブロックデータを読み出したか？
No
Yes
エンド

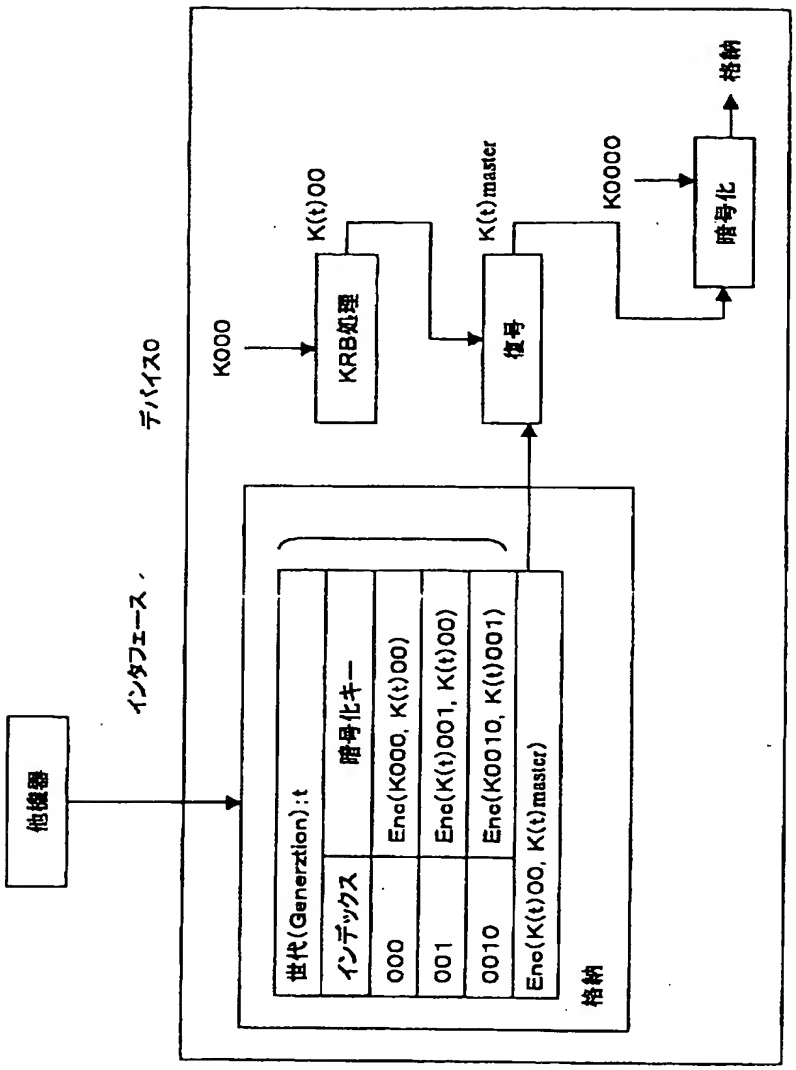
【図３６】


3600
110
3801
モデム
電話回線
ディジタル信号
120
入出力I/F
170
CPU
140
130
入出力I/F
141
MPEG
コーデック
180
アナログ信号
A/D, D/A
コンバータ
メモリ
300
TS
処理手段
210
195
150
暗号処理手段
(ex. 暗号LSI)
記録媒体I/F
記録媒体

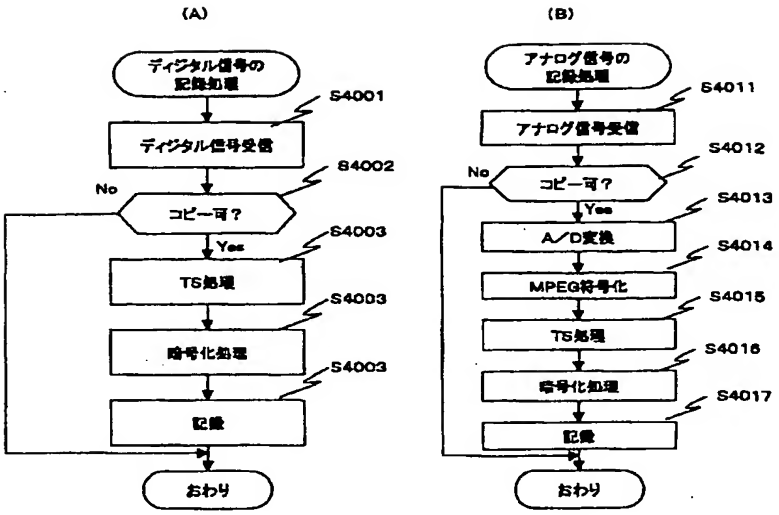
【図３９】


世代(Generation):t
インデックス
暗号化キー
000
Enc(K000, K(t)00)
001
Enc(K(t)001, K(t)00)
0010
Enc(K0010, K(t)001)
Enc(K(t)00, K(t)master)
記録媒体
世代(Generation):t
インデックス
暗号化キー
000
Enc(K000, K(t)00)
001
Enc(K(t)001, K(t)00)
0010
Enc(K0010, K(t)001)
Enc(K(t)00, K(t)master)
記憶手段
デバイスD

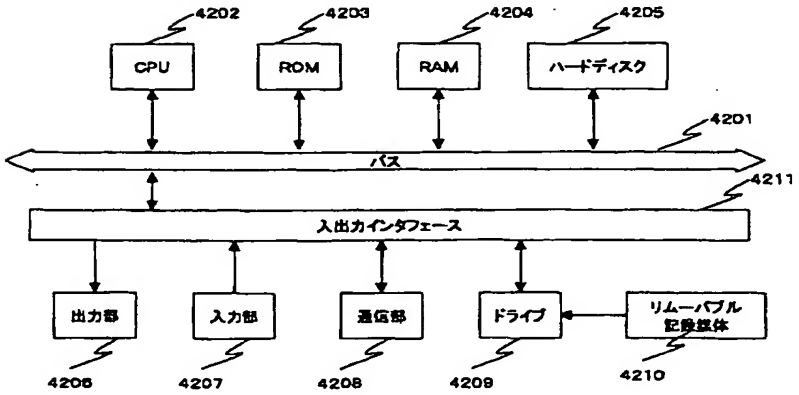
【図３７】


他機器
インタフェース
デバイス0
K000
KRB処理
K(t)00
暗号
K(t)master
K0000
暗号化
格納
世代(Generation):t
インデックス
暗号化キー
000
Enc(K000, K(t)00)
001
Enc(K(t)001, K(t)00)
0010
Enc(K0010, K(t)001)
Enc(K(t)00, K(t)master)
格納

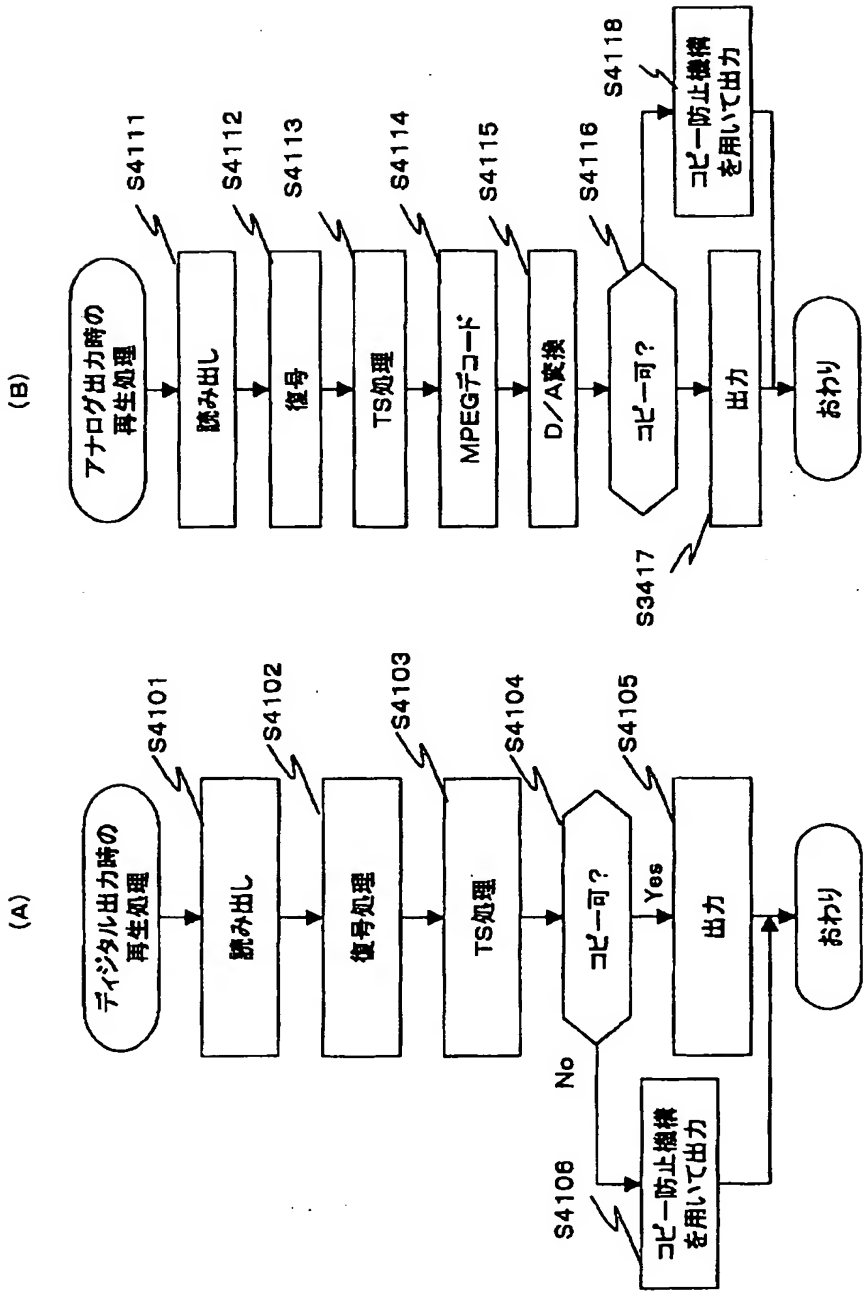
【図４０】


(A)
ディジタル信号の記録処理
S4001
ディジタル信号受信
S4002
No
コピー可？
Yes
S4003
TS処理
S4003
暗号化処理
S4003
記録
おわり
(B)
アナログ信号の記録処理
S4011
アナログ信号受信
S4012
No
コピー可？
Yes
S4013
A/D変換
S4014
MPEG符号化
S4015
TS処理
S4016
暗号化処理
S4017
記録
おわり

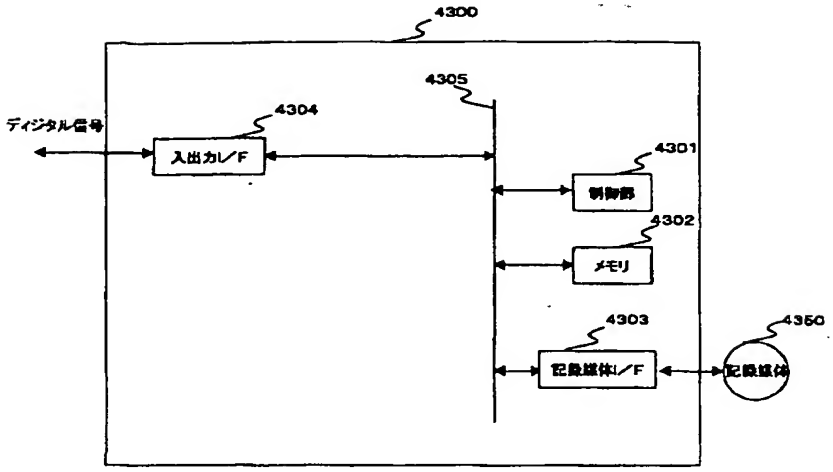
【図４２】


4202
CPU
4203
ROM
4204
RAM
4205
ハードディスク
4201
バス
4211
入出力インタフェース
出力部
入力部
通信部
ドライブ
リムーバブル記録媒体
4206
4207
4208
4209
4210

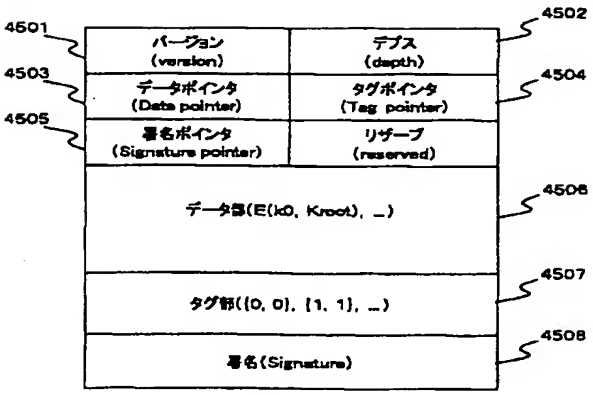
【図41】


(A)
ディジタル出力時の再生処理
S4101
読み出し
S4102
復号処理
S4103
TS処理
S4104
コピー可?
No
Yes
S4105
出力
おわり
S4106
コピー防止機構を用いて出力
(B)
アナログ出力時の再生処理
S4111
読み出し
S4112
復号
S4113
TS処理
S4114
MPEGデコード
S4115
D/A変換
S4116
コピー可?
S4118
コピー防止機構を用いて出力
出力
S3417
おわり

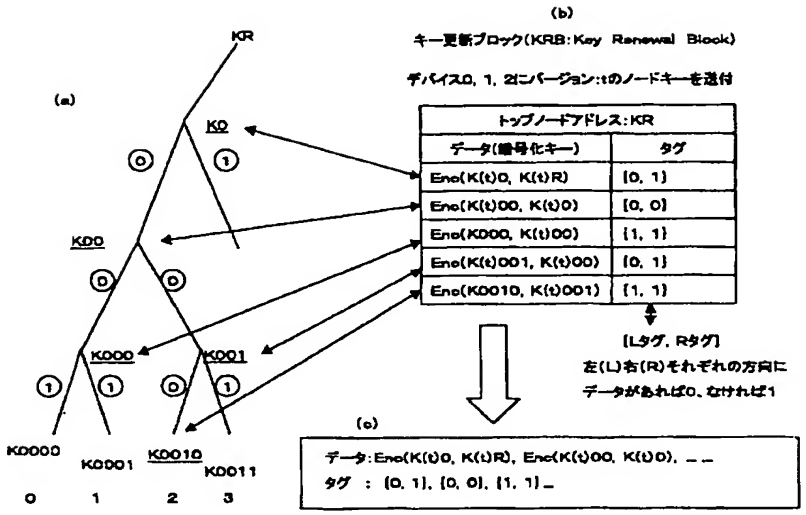
【図４３】


4300
4305
ディジタル信号
4304
入出力I／F
4301
制御部
4302
メモリ
4303
4350
記録媒体I／F
記録媒体

【図４５】


4501
4502
バージョン
(version)
デプス
(depth)
4503
データポインタ
(Data pointer)
4504
タグポインタ
(Tag pointer)
4505
署名ポインタ
(Signature pointer)
リザーブ
(reserved)
4506
データ部(E(k0, Kroot), ...)
4507
タグ部([0, 0], [1, 1], ...)
4508
署名(Signature)

【図４６】



フロントページの続き

(51) Int. Cl. 7	識別記号	F I	テーマコード（参考）
		H04N 5/91	P

(72)発明者　石黒　隆二
東京都品川区北品川６丁目７番35号　ソニー株式会社内
(72)発明者　光澤　敦
東京都品川区北品川６丁目７番35号　ソニー株式会社内
(72)発明者　大石　丈於
東京都品川区北品川６丁目７番35号　ソニー株式会社内

Ｆターム(参考)　5B017 AA03 AA06 BA07 CA09
5C053 FA24 GB37 HA40 JA01 JA24
JA30 KA05 KA24 KA25 LA14
5D044 AB05 AB07 BC06 CC06 DE50
GK17 HL02 HL08
5J104 AA13 AA16 AA34 EA07 EA18
EA26 NA02 NA11 NA12